TEKNILLINEN KORKEAKOULU

Sähkö- ja Tietoliikennetekniikan osasto

Teemu Ylhäisi

Mobiiliyhteydet yrityksen tietoverkkoon

Diplomityö, joka on jätetty opinnäytetyönä tarkastettavaksi

diplomi-insinöörin tutkintoa varten Espoossa 28.11.2003

Työn valvoja Professori Heikki Hämmäinen

Työn ohjaaja DI Mika Sarén

TEKNILLINEN KORKEAKOULU **Diplomityön tiivistelmä**

Tekijä:	Teemu Ylhäisi
Työn nimi:	Mobiiliyhteydet yrityksen tietoverkkoon
Päivämäärä:	28.11.2003 **Sivumäärä:** 103
Osasto:	Sähkö- ja tietoliikennetekniikan osasto
Professuuri:	S-38 Tietoverkkotekniikka
Työn valvoja:	Professori Heikki Hämmäinen
Työn ohjaaja:	DI Mika Sarén

Työn tavoitteena oli tarkastella yrityksen mobiiliyhteyksien toteutusvaihtoehtoja. Yrityksen tietoverkon palvelut ovat tärkeitä työvälineitä, joita voidaan hyödyntää nykyistä tehokkaammin muodostamalla langattomien tietoverkkojen kautta suojattuja yhteyksiä yrityksen tietoverkkoon. Langattomien tietoverkkojen avulla yritysverkon palveluita voidaan käyttää perinteisten toimipisteiden ulkopuolella paikasta riippumatta.

Työ jakautuu kahteen osaan: teoriaosaan ja yrityksen mobiiliyhteyksien toteutusvaihtoehtojen arviointiin. Teoriaosassa käsitellään pakettikytkentäisiä matkapuhelinverkkoja ja langattomia lähiverkkoja niiden tekniikoiden ja käyttömahdollisuuksien kannalta sekä yritysverkkojen tietoturvamekanismeja ja virtuaaliverkkoteknologioita. Mobiiliyhteyksien arvioinnissa luotiin joukko kriteerejä, joiden avulla mobiiliyhteyksien toteutusvaihtoehtoja voidaan arvioida tietoturvan, kustannusten ja yrityksen ja loppukäyttäjän kokeman hyödyn kannalta. Kriteereiden perusteella arvioitiin seitsemää eri arkkitehtuurivaihtoehtoa.

Arvioinnin perusteella todettiin, että mikään esitetyistä arkkitehtuurivaihtoehdoista ei tarjoa yleispätevää ratkaisua yritysten mobiiliyhteydeksi. Ratkaisuiden arvioinnin lähtökohdaksi on otettava yrityksen yksilölliset tarpeet ja käytettävä niitä lähtökohtana arviointiprosessissa, jossa voidaan hyödyntää tässä työssä luotuja kriteerejä.

Avainsanat: VPN, IPsec, GPRS, WLAN, yritysverkko

HELSINKI UNIVERSITY OF TECHNOLOGY **Abstract of the Master's Thesis**

Author:	Teemu Ylhäisi
Name of the Thesis:	Mobile Access to Corporate Intranet
Date:	November 28th, 2003 **Number of pages:** 103
Department:	Department of Electrical and Communications Engineering
Professorship:	S-38 Networking Technology
Supervisor:	Professor Heikki Hämmäinen
Instructor:	Mika Sarén, M.Sc. (Tech.)

The object of this thesis was to evaluate different solutions for mobile access to corporate networks. Essential tools and data sources in corporate networks can be used more efficiently when wireless networks are used for connecting single users to a corporate network. Furthermore, wireless networks enable people to work regardless of time and location.

This thesis has two parts. The first part is theoretical and the second is an evaluation of the solutions for mobile access to corporate networks. The theoretical part covers the following subjects: Packet switched mobile networks, wireless local area networks, corporate security solutions and virtual private network technologies. A set of criteria was created and used for the evaluation on seven mobile access architectures.

Based on the evaluation, it can be stated that none of the seven solutions presented in this thesis will provide a universal solution for every mobile access to corporate networks. Individual requirements in a company must be the basis for the evaluation in a corporation. The criterion created in this thesis can be used in evaluation processes in companies'.

Keywords: VPN, IPsec, GPRS, WLAN, corporate network

ALKULAUSE

Haluan kiittää tämän työn valvojaa Professori Heikki Hämmäistä rakentavista keskusteluista ja ohjeista työn eri vaiheissa.

Kiitos työni ohjaajalle Mika Sarénille saamistani kommenteista ja parannusehdotuksista, sekä mahdollisuudesta tehdä tämä työ Radiolinjan Teknologiakeskuksessa. Kiitoksia myös Jani Krigsmanille ja Sari Pekkariselle sekä muille kollegoille Radiolinjalla avusta ja kommenteista.

Lopuksi haluan kiittää Elinaa kaikesta tuesta ja avusta, jota olen saanut opintojeni aikana ja tehdessäni tätä työtä.

Espoossa, 28.11.2003

Teemu Ylhäisi

SISÄLLYSLUETTELO

KUVALUETTELO

SYMBOLI- JA LYHENNELUETTELO

3DES	Triple Data Encryption Standard
3G	3rd Generation
8-PSK	Octagonal Phase Shift Keying
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
APN	Access Point Name
ATM	Asynchronous Transfer Mode
AuC	Authentication Centre
BG	Border Gateway
BS	Base Station
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CDR	Charging Data Record
COA	Care Of Address
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data for GSM Evolution
EIR	Equipment Identity Register
ESP	Encapsulating Security Payload
FA	Foreign Agent
GERAN	GSM/EDGE Radio Access Network
GGSN	GPRS Gateway Support Node
GMSC	Gateway Mobile Switching Center
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio System
GR	GPRS Register

GRE	Generic Routing Encapsulation
GRX	GPRS Roaming eXchange
GSM	Global System for Mobile Communication
GSMA	GSM Association
GTP	GPRS Tunneling Protocol
HA	Home Agent
HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISAKMP	Internet Security Association and Key Management Protocol
L2F	Layer Two Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MCC	Mobile Country Code
MGW	Media Gateway
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
MTU	Maximum Transmission Unit
NAS	Network Access Server
NAT	Network Address Translation
NSS	Network Subsystem
OSI	Open System Interconnection
PCMCIA	Personal Computer Memory Card International Association

PCU	Packet Control Unit
PDA	Personal Digital Assistant
PLMN	Public Land Mobile Network
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RFC	Request for Comments
RNC	Radio Network Controller
SA	Security Association
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SPI	Security Parameter Index
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TRAU	Transcoder and Rate Adaption Unit
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Radio Access Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
VLR	Visitor Location Register
VPN	Virtual Private Network

1 JOHDANTO

1.1 Tausta

Monet päivittäiseen työntekoon liittyvät työvälineet ja tiedot, kuten sähköposti, kalenteri, tiedostot ja tietokannat, ovat sidoksissa yrityksen tietoverkkoon. Vaikka kannettavat tietokoneet, kämmentietokoneet ja älypuhelimet mahdollistavatkin paikallisen tietojenkäsittelyn sijainnista riippumatta ilman päätelaitteen ja yritysverkon välisiä tietoliikenneyhteyksiä, ei yritysverkossa olevia työkaluja voida hyödyntää parhaalla mahdollisella tavalla. Työskentelykulttuurien muuttuessa etätyöskentely lisääntyy, eikä perinteinen työpaikallakaan tehtävä työ ole välttämättä kiinteästi sidoksissa tiettyyn työpisteeseen. Yrityksen työntekijöiden tarpeet käyttää yrityksen tietoverkon sisäisiä palveluja ja hyödyntää siellä olevaa tietoa kasvavat. Tästä johtuen yritykset hakevatkin nyt ratkaisuja, joiden avulla työntekijät voivat hyödyntää kannettavien päätelaitteiden tietojenkäsittelykapasiteetin lisäksi myös yrityksen tietoverkon palveluita ja tietoja.

Yrityksen tietoverkossa olevat palvelut ovat tärkeä osa työntekijöiden työvälineitä ja niitä voidaan hyödyntää vain, jos työntekijöillä on yhteys yrityksen tietoverkkoon. Yrityksen lähiverkot ovat perinteisesti tarjonneet tietoverkon palveluita rajallisella alueella, yrityksen toimitiloissa. Langattomien tietoliikenneyhteyksien avulla yrityksillä on mahdollisuus tarjota työntekijöilleen tietoverkon palveluja sijainnista riippumatta.

Pakettikytkentäiset matkapuhelinverkot kehittyvät tarjoamaan entistä tehokkaampaa langatonta tiedonsiirtoa, jota voidaan hyödyntää Suomen lisäksi myös ulkomailla [1]. Pakettikytkentäisten matkapuhelinverkkojen lisäksi langattomien lähiverkkojen käyttö lisääntyy jatkuvasti ja julkisten verkkojen määrä kasvaa kokoajan [2]. Pakettikytkentäiset matkapuhelinverkot ja langattomat lähiverkot tarjoavat

tietoliikenneyhteydet, joita yritykset voivat käyttää työntekijöidensä mobiiliyhteyksien perustana.

Sekä yrityksen lähiverkossa että ulkopuolisissa verkoissa välitettävään tietoliikenteeseen kohdistuu tietoturvauhkia, jotka muodostavat yrityksen kannalta tietoturvariskin. Yritysmaailmassa käsitellään usein salaisia tai luottamuksellisia tietoja, joiden joutuminen yrityksen ulkopuolelle saattaa olla vahingollista. Salaisia tai luottamuksellisia tietoja voidaan välittää tietoverkoissa esimerkiksi sähköpostin liitetiedostoina, jolloin tietoturvariski koskee myös käytettäviä tietoliikenneyhteyksiä [3].

Välitettäessä tietoa ulkopuolisten verkkojen kautta, on tietoliikenteeseen kohdistuva uhka sisäisessä verkossa välitettyyn liikenteeseen kohdistuvaa uhkaa huomattavasti suurempi. Muodostettaessa mobiiliyhteyksiä yrityksen tietoverkkoon tietoliikenne kulkee useimmissa tapauksissa ulkopuolisten verkkojen, kuten Internetin tai tietoliikenneoperaattorin tietoverkon kautta [4]. Käytettäessä ulkopuolisia tietoverkkoja yrityksen sisäisen tietoliikenteen välityksessä, on näiden verkkojen aiheuttamat tietoturvauhat arvioitava ja tarpeelliset suojausmekanismit otettava käyttöön tiedon luottamuksellisuuden takaamiseksi.

Käytettäessä mobiiliyhteyksiä yrityksen tietoverkossa, tarvitaan ratkaisuja, jotka täyttävät sekä mobiiliyhteydelle asetetut vaatimukset liikkuvuuden ja tiedonsiirtokapasiteetin suhteen että yrityksen tietoliikenteen tietoturvalle asetetut vaatimukset. Virtuaaliverkkoteknologioilla yhdistetään toisistaan erillisiä tietoverkkoja ja tietokoneita verkkotopologian kannalta loogisesti yhdeksi verkoksi. Virtuaaliverkkoteknologioita voidaan käyttää suurten lähiverkkojen yhdistämisessä, mutta myös yksittäisten tietokoneiden liittämisessä osaksi yritysverkkoa. [4]

1.2 Ongelman määrittely

Useat eri tietoliikenneoperaattorit tarjoavat omia tuotteitaan yrityksille, jotka ovat suunnittelemassa uuden tietoliikenneratkaisun käyttöönottoa. Tuotteet eroavat toisistaan ominaisuuksien, laitteistojen ja hinnoittelun suhteen, joten niiden keskinäinen arviointi on monimutkainen tehtävä. Jotta eri tuotteiden välinen arviointi voitaisiin suorittaa tehokkaasti, on määriteltävä selkeät vaatimukset, selvitettävä eri vaihtoehdot, arvioitava näitä vaihtoehtoja ja tehtävä lopullinen valinta. Yrityksen kannalta prosessi on monimutkainen ja ilman systemaattista menettelytapaa valinnassa saatetaan painottaa epäolennaisia ominaisuuksia, jolloin yritys ei välttämättä löydä itselleen sopivinta ratkaisua.

1.3 Tavoitteet

Tässä työssä tarkastellaan ratkaisuja, joiden avulla yrityksen työntekijät voivat muodostaa mobiiliyhteyksiä yrityksen tietoverkkoon. Yritysverkon mobiiliyhteydet koostuvat langattoman tiedonsiirron mahdollistavista matkapuhelinverkoista ja langattomista lähiverkoista sekä yhteyksien suojaamisessa käytetyistä virtuaaliverkkoteknologioista. Työssä kuvataan erilaisia arkkitehtuurivaihtoehtoja yrityksen mobiiliyhteyksien toteuttamiseksi.

Työn tavoitteena on luoda joukko kriteerejä, joiden perusteella esiteltyjä arkkitehtuurivaihtoehtoja voidaan arvioida useista eri näkökulmista. Kriteereiden valinnassa on otettava huomioon eri toimijoiden, kuten palveluita käyttävän yrityksen, sekä palveluita tuottavan tietoliikenneoperaattorin näkökulmat.

Työn toisena tavoitteena on arvioida eri arkkitehtuurivaihtoehtoja laadittujen kriteerien perusteella ja näin osoittaa eri arkkitehtuurien heikkoudet, vahvuudet ja käyttömahdollisuudet.

1.4 Työn rajaus

Yritysten mobiiliyhteysratkaisut koostuvat langattomista tietoliikenneverkoista ja tietoturvaa parantavista ratkaisuista. Tässä työssä käsitellään kahden tyyppisiä langattomia tietoliikenneverkkoja, eli pakettikytkentäisiä matkapuhelinverkkoja ja langattomia lähiverkkoja. Yrityksille tarjottavien mobiiliyhteysratkaisuiden merkittävin lisäarvo langattoman tietoliikenneyhteyden lisäksi on välitettävän liikenteen suojaus. Työssä käsitellään yritysverkkojen tietoturvamekanismeja ja virtuaalisissa yksityisverkoissa käytettäviä tunnelointiprotokollia, joiden avulla mobiiliverkoissa välitettävä liikenne suojataan.

1.5 Diplomityön rakenne

Työn toisessa kappaleessa esitellään pakettikytkentäisten matkapuhelinverkkojen arkkitehtuuria ja toimintaa. Kappaleessa keskitytään GPRS-verkon (General Packet Radio System) elementteihin ja niiden toimintaan, sekä esitellään EDGE- (Enhanced Data for GSM Evolution) ja UMTS-verkkojen (Universal Mobile Telecommunications System) toiminta lyhyesti. Työn kolmannessa kappaleessa käsitellään langattomia lähiverkoja tarkastelemalla niiden standardeja, verkkoarkkitehtuureja ja käyttötarkoituksia.

Neljännessä kappaleessa tarkastellaan yritysverkkojen tietoturvamekanismeja, jotka ovat merkittäviä virtuaalisten yksityisverkkojen ja mobiiliverkkojen kannalta. Kappaleessa käsitellään tietoturvaa yleisesti sekä esitellään pakettikytkentäisten matkapuhelinverkkojen ja langattomien lähiverkkojen tietoturvaominaisuuksia ja riskejä. Toinen, kolmas ja neljäs kappale muodostavat teoriapohjan virtuaalisten yksityisverkkojen tarkastelulle ja niiden käytölle mobiiliverkoissa

Viides kappale käsittelee virtuaalisten yksityisverkkojen toteutustapoja ja arkkitehtuureja. Kappaleessa esitellään sekä pakettikytkentäisissä matkapuhelinverkoissa että langattomissa lähiverkoissa käytettäviä ratkaisuja, joilla

voidaan toteuttaa yritysverkon mobiiliyhteyksiä. Kappaleessa käsitellään virtuaalisiin yksityisverkkoihin liittyviä protokollia ja tekniikoita sekä yritysverkoissa käytettäviä mobiilipäätelaitteita.

Kuudennessa kappaleessa luodaan yrityksen mobiiliyhteyksien arviointiin sopivat kriteerit ja käytetään näitä kriteerejä viidennessä kappaleessa esiteltyjen arkkitehtuurivaihtoehtojen arviointiin. Kriteerit on työssä jaettu kolmeen luokkaan, jotka ovat. Seitsemännessä kappaleessa esitetään johtopäätökset, joihin luotujen kriteerien ja arkkitehtuurien arvioinnin perusteella on päädytty.

2 PAKETTIKYTKENTÄISET MATKAPUHELINVERKOT

Tässä kappaleessa esitellään yritysverkon mobiiliyhteyksien käytön kannalta oleellisimmat matkapuhelinverkkoteknologiat, jotka ovat jo nyt käytössä oleva GSM-verkon (Global System for Mobile Communications) laajennukset GPRS ja EDGE sekä Euroopassa käyttöön tuleva kolmannen sukupolven matkapuhelinverkko UMTS.

Yrityksen tietoverkkoon on mahdollista muodostaa pakettikytkentäisten yhteyksien lisäksi myös piirikytkentäisiä mobiiliyhteyksiä. Piirikytkentäisten datayhteyksiä voidaan muodostaa kahdella eri tekniikalla; GSM-data ja HSCSD (High Speed Circuit Switched Data). GSM-järjestelmän piirikytkentäinen datasiirto toimii käyttäjän kannalta kuten kiinteän verkon modeemiyhteys ja saavutettava datanopeus on maksimissaan 9,6 kb/s. HSCSD-tekniikalla otetaan radioverkossa käyttöön useita aikavälejä yhtä käyttäjää kohti, jolloin saavutetaan maksimissaan 57,6 kb/s siirtonopeus [5]. Tässä työssä ei käsitellä tarkemmin mobiiliverkkojen piirikytkentäisiä datapalveluita, koska GPRS:n ja muiden pakettikytkentäisten datasiirtopalveluiden kehittyessä ja yleistyessä piirikytkentäisten langattomien datapalveluiden merkitys ole yhtä suuri, kuin aikaisemmin. Lisäksi yritysverkkojen mobiiliyhteyksillä välitettävä liikenne on pääosin IP-pohjaista (Internet Protocol), jonka välittämiseen pakettikytkentäiset tekniikan soveltuvat piirikytkentäisiä tekniikoita paremmin.

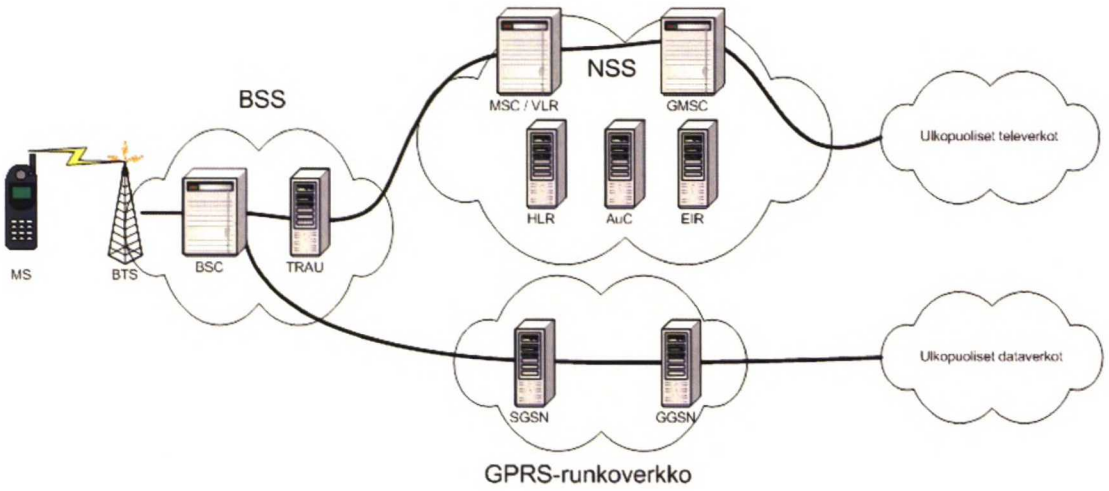
2.1 General Packet Radio Service (GPRS)

GSM:n pakettikytkentäinen datapalvelu GPRS on GSM-järjestelmän laajennus. GSM-verkon kautta välitettävät datapalvelut ovat olleet käyttäjän kannalta ennen GPRS:n käyttöönottoa piirikytkentäisiä, eli yhteys on muodostettu ja sitä on ylläpidetty, vaikka varsinaista liikennevirtaa ei olisikaan jatkuvasti. Piirikytkentäisen datasiirron käyttöä rajoittavana tekijänä on ollut yhteysaikaan perustuva laskutus, jonka takia piirikytkentäiset datapalvelut ovat olleet moniin tarkoituksiin liian kalliita. GPRS on sen sijaan tarkoitettu purskeisen, IP-protokollan mukaisen datan välitykseen. Vaikka yhteys

olisi loogisesti muodostettu päätelaitteen ja esimerkiksi Internet-verkon välille, palvelussa ei ole tarpeen varata fyysistä yhteyttä jatkuvasti. Fyysinen yhteys on aktiivinen ainoastaan datasiirron aikana. [6] Koska purskeisen datan välityksessä radioyhteyttä varataan ainoastaan liikennettä lähetettäessä tai vastaanotettaessa, voidaan laskutusperusteenakin käyttää välitetyn datan määrää yhteysajan sijasta [7].

Piirikytkentäinen osa GSM-verkosta sisältää verkkoelementtejä, jotka ovat sekä piirikytkentäisen että pakettikytkentäisen osan käytössä. Kotirekisteri (HLR, Home Location Register) on tietokanta, jonka tehtävänä on kerätä ja säilyttää tilaaja- ja laskutustietoja sekä tietoa käyttäjille aktivoiduista lisäpalveluista. Jokainen käyttäjä on rekisteröitynyt yhteen kotirekisteriin, jossa kyseisen tilaajan tietoja säilytetään. Vierailijarekisteri (VLR, Visitor Location Register) ylläpitää tietoja tietyn keskuksen alueella olevista matkapuhelimista. Vierailijarekisterit saavat tilaajien tiedot jokaisen tilaajan omalta kotirekisteriltä. Jokaiseen matkapuhelimeen on tallennettu laitetunnus, jonka avulla päätelaitteet voidaan tunnistaa. Laitetunnusrekisteri (EIR, Equipment Identity Register) on tietokanta, joka sisältää päätelaitteiden laitetunnuksia. Laitetunnusrekisteriä käytetään varastettujen ja tyyppihyväksymättömien laitteiden käytön estämiseen. [8]

GPRS:n myötä GSM-verkkoon on tehty päivityksiä olemassa oleviin verkkoelementteihin sekä lisätty GPRS-verkkoon kuuluvia täysin uusia verkko-elementtejä. GPRS:n käyttöönoton myötä GSM-verkkoon tehdyt päivitykset ovat pääosin ohjelmistopäivityksiä verkon rekistereihin ja tukiasemaohjaimiin. Uusia verkkoelementtejä piirikytkentäiseen GSM-verkkoon verrattuna ovat operointisolmu (SGSN, Serving GPRS Support Node), yhdyskäytäväsolmu (GGSN, Gateway GPRS Support Node), GPRS-rekisteri (GR, GPRS Register), pakettiohjausyksikkö (PCU, Packet Control Unit) sekä erillinen GPRS-runkoverkko. [6][8] Kuvassa 1 on esitetty GPRS-verkko tämän työn kannalta oleellisessa laajuudessa.



Kuva 1 GPRS-verkko [9]

2.1.1 GPRS-runkoverkko

GPRS-runkoverkon tehtävänä on yhdistää GPRS:n palvelevat solmut ja tarjota yhteyksiä muihin PLMN-verkkoihin (Public Land Mobile Network). GPRS-runkoverkko on joko IP- tai IP over ATM-verkko (Asynchronous Transfer Mode), joka koostuu reitittimistä ja kytkimistä. [8] GPRS-runkoverkko toimii omana hallinnollisena alueenaan, jossa toimivat IP-verkon peruspalvelut, kuten nimipalvelin (DNS, Domain Name Server), DHCP-palvelin (Dynamic Host Configuration Protocol), RADIUS-autentikointipalvelin (Remote Access Dial-In User Service) ja palomuurit. GPRS-verkkovierailu on toteutettu reunayhdyskäytävällä (BG, Border Gateway), joka yhdistää GPRS-verkot toisiinsa välittämällä liikennettä GRX-verkon (GPRS Roaming eXchange) kautta.

GPRS sisältää monia runkoverkon osia, joita ei ole käytetty perinteisissä GSM-verkoissa. Yksi näistä menetelmistä on Frame Relay-verkon käyttö GSM:n tukiasemajärjestelmän ja GPRS-verkon välillä. Sama yhteysväli on toteutettu ATM-verkolla UMTS-radiojärjestelmän ja GPRS-verkon välillä. Toinen uudistus GPRS-verkossa on IP-protokollan käyttö GPRS-runkoverkossa. [6]

2.1.2 Serving GPRS Support Node (SGSN)

Matkapuhelinverkon kannalta SGSN on GPRS-verkossa samalla loogisella tasolla, kuin GSM-verkossa MSC (Mobile Switching Center), tehtävänään seurata yksittäisten GPRS-päätelaitteiden sijaintia. SGSN ylläpitää tietoa päätelaitteiden sijainnista solun ja reititysalueen tarkkuudella riippuen päätelaitteen liikkuvuuden hallintatilasta. SGSN huolehtii myös käyttäjien tunnistamiseen, suojaukseen ja pääsynhallintaan liittyvistä toiminnoista. GPRS-yhteys on siten salattu päätelaitteen ja SGSN:n välillä. [6] GPRS-verkon tietoturvaa käsittelen laajemmin kappaleessa 4.2.1.

Edellisten toimintojen lisäksi SGSN:n kautta operaattori kerää tarpeellisia laskutustietoja GPRS-yhteyksistä, eli SGSN:n kautta muodostetaan laskutustikettejä (CDR, Charging Data Record). Tärkein laskutukseen vaikuttava seikka on radiorajapinnan resurssien käyttö, eli kuinka paljon käyttäjä hyödyntää radioverkon siirtokapasiteettia. GPRS-järjestelmässä voidaan laskuttaa lähetetyn ja vastaanotetun käyttäjän datan mukaan, vaikka yhteys olisi loogisesti muodostettuna kauemminkin. [6]

2.1.3 Gateway GPRS Support Node (GGSN)

GGSN mahdollistaa datasiirron ulkopuolisten dataverkkojen ja GPRS-verkon välillä. GGSN on kytketty SGSN:ään IP-pohjaisen GPRS-runkoverkon kautta. Ulkopuolisille verkoille GGSN näkyy käytännössä joko IP-verkon reitittimenä tai X.25-verkon solmuna. GGSN on GSM- tai UMTS-verkon ja ulkopuolisen dataverkon rajapinnassa, ja sen toiminta verkon sisällä on sama sekä GSM-verkon, että UMTS-verkon kannalta. [6]

GGSN:n yhtenä tehtävänä on pitää yllä standby-tilassa olevien päätelaitteiden sijaintitietoa SGSN:n tarkkuudella, eli tietoa siitä, mikä SGSN palvelee tiettyä päätelaitetta. Tätä sijaintitietoa ylläpidetään käyttäjän kotiverkon GGSN:ssä päätelaitteen ollessa kotiverkossa tai vieraillessa muussa GPRS-verkossa. Jos liikkuvuuden hallinta on ready-tilassa, SGSN tietää päätelaitteen sijainnin solun tarkkuudella. Vaikka GGSN on periaatteessa tavanomaisen kiinteän verkon reititintä

vastaava elementti, on GPRS- ja kiinteän verkon välillä merkittävä ero liikkuvuuden hallinnan suhteen. Siksi normaaleista reitittimistä poiketen GGSN:n on kyettävä reitittämään datayhteydet liikkuvassa ympäristössä. [6]

Yhteen GGSN-elementtiin voi olla kytkeytyneenä yksi tai useampia SGSN-elementtejä GPRS-runkoverkon kautta. Datapaketit SGSN:n ja GGSN:n välillä tunneloidaan erityisellä GTP-protokollalla (GPRS Tunneling Protocol). [6]

Kuten SGSN, myös GGSN kykenee keräämään laskutukseen liittyvää informaatiota eli laskutustikettejä pakettidatayhteyksistä. Erona on se, että GGSN pystyy keräämään erityisesti ulkopuolisiin dataverkkoihin liittyvää laskutustietoa. [6]

2.1.4 Access Point Name (APN)

APN (Access Point Name) on looginen tapa nimetä käyttäjille tarjottavia GPRS-palveluita. APN:n tehtävänä on eritellä ja reitittää käyttäjien liikenne käytettävän palvelun vaatimalla tavalla. Käyttäjän muodostaessa GPRS-yhteyttä valitaan, tai on etukäteen valittu tietty APN, jonka perusteella GPRS-yhteys muodostetaan.

APN-osoite on viittaus tietyn GPRS-verkon GGSN:ään ja mobiiliverkkojen verkkovierailun toteuttamiseksi APN-osoite muunnetaan GPRS-runkoverkossa olevien DNS-palveluiden avulla vastaavaksi GGSN:n IP-osoitteeksi [10]. APN-osoite saattaa viitata käytettävän verkon GGSN:ään tai käyttäjän kotiverkon GGSN:ään. APN osoite koostuu kahdesta osasta: verkkotunnisteesta ja operaattoritunnisteesta.

- APN-osoitteen verkkotunniste määrittelee mihin GGSN:n välittämään palveluun kyseinen APN-osoite liittyy. Tämä osa APN-osoitetta on pakollinen
- APN-osoitteen operaattoritunniste, joka määrittelee minkä operaattorin mobiiliverkossa APN-osoitteen viittaama GGSN sijaitsee. Operaattoritunniste ei ole pakollinen osa APN-nimeä. [11]

APN-osoitteiden verkko- ja operaattoritunnisteet koostuvat Internetosoitteiden tapaan pisteillä erotetuista osista. GSMA (GSM Association) suosittelee, että käytetyt APN-osoitteen verkkotunnukset muodostetaan operaattorin rekisteröimistä Internetnimistä (domain name). [11] Esimerkiksi VoiceStream Wirelessin käyttämä WAP-APN (Wireless Application Protocol) on muotoa

wap.voicestream.com

Vaikka operaattoritunniste ei ole pakollinen osa APN-nimeä, on jokaisella operaattorilla oltava uniikki operaattoritunniste, jotta sitä voidaan käyttää tarvittaessa. APN-osoitteen operaattoritunnistetta käytetään verkkovierailutilanteissa, joissa asiakkaat halutaan ohjata käyttämään kotiverkon GGSN:n välittämiä palveluita, eikä käyttäjän tarvitse käyttää vierailtavan verkon GGSN:n tarjoamia palveluita.

APN-osoitteen operaattori tunniste koostuu kolmesta eri osasta, joista viimeinen on kaikilla operaattoreilla *gprs*. Ensimmäinen ja toinen osa muodostuvat operaattorille määritellyn IMSI-numeron (International Mobile Subscriber Number) mukaan siten, että ensimmäinen osa muodostuu operaattorille määritellystä verkkokoodista (MNC, Mobile Network Code) ja toinen operaattorin maatunnuksesta (MCC, Mobile Country Code). VoiceStream Wirelessin verkkokoodi on 026 ja maatunnus 310, jolloin APN-osoitteen operaattoritunniste olisi [10][11]:

*mnc*026.*mcc*310.*gprs*

Yhdistämällä APN-osoitteen verkko- ja operaattoritunnisteet muodostuu APN-osoite kokonaisuudessaan.

$$\underbrace{wap.voicestream.com}_{\text{verkkotunniste}}.\underbrace{mnc026.mcc310.gprs}_{\text{operaattoritunniste}}$$

APN-osoitteen perusteella päätelaite pyytää haluttuja palveluja oikealta GGSN:ltä ja GGSN tarjoaa käyttäjälle tiettyjä ennalta määriteltyjä palveluita ja yhteyksiä. Juuri APN-

osoitteiden avulla GPRS-yhteyksiä voidaan tarjota differentoituja palveluita, jotka vastaavat käyttäjien tarpeita. Käyttämällä useita APN-osoitteita eritavoilla, voidaan vaikuttaa seuraaviin tekijöihin:

- Käyttäjien liikenteen reititys
- GPRS-yhteyden laskutus
- Käyttäjien tunnistus.

Pakettien reititystä voidaan tehdä APN-osoitekohtaisesti, jolloin tietyn APN:n kautta kulkeva liikenne reititetään poikkeavasti [11]. Reitityksen muokkaamista voidaan hyödyntää muodostettaessa yhteyksiä yritysverkkoon sallimalla tietystä APN:stä tuleva liikenne ainoastaan tiettyyn osoitteeseen tai osoiteavaruuteen. Tämä osoite voi olla esimerkiksi yrityksen yhdyskäytäväpalvelin tai yrityksen tietoverkon IP-osoiteavaruus. Myös muiden rajattujen palveluiden tarjoaminen APN-kohtaisesti on mahdollista reitityksen hallinnan avulla.

Eri APN-osoitteiden käyttöä voidaan laskuttaa eri tavoilla. Internet-APN:n laskutus voi perustua välitetyn datan määrään ja esimerkiksi MMS-palveluiden (Multimedia Messaging Service) laskutuksessa välitetyn datan määrää ei nykyisellään huomioida, vaan laskutusperusteena käytetään ainoastaan lähetettyjen viestien määrä. [7] Eri laskutusvaihtoehdoilla mahdollistetaan erilaiset palvelumallit ja erilaisten palveluiden tarjoaminen.

Käyttäjien tunnistusta voidaan suorittaa APN-kohtaisesti, jolloin voidaan hallita APN-osoitteiden käyttäjäryhmiä. Tätä ominaisuutta voidaan hyödyntää esimerkiksi tarjottaessa yrityskohtaisia APN-osoitteita, jolloin ainoastaan yrityksen liittymistä pystytään muodostamaan yhteyksiä kyseiseen APN-osoitteeseen.

Yhteyttä muodostettaessa päätelaite lähettää SGSN:lle pyynnön palvelun aktivoimisesta. SGSN selvittää käyttäjän kotirekisteristä, onko käyttäjä oikeutettu kytkeytymään tiettyyn

APN:ään. HLR:ssä on määritetty ne APN:t, joita käyttäjä saa käyttää, tai sallittu villikortti-APN:n (APN = *) käyttö, jolloin käyttäjä on oikeutettu käyttämään kaikkia verkon tarjoamia APN-osoitteita. Oikeutuksen tarkistuksen jälkeen SGSN aloittaa oikean GGSN:n haun. [11]

Jos käyttäjä on oikeutettu pyydetyn APN:n käyttöön, SGSN lähettää nimipalvelukyselyn, jonka tarkoitus on selvittää kyseistä APN:ää vastaava IP-osoite. Käytettävän GPRS-verkon nimipalvelin vastaa kyselyyn, jos haluttu APN on samassa verkossa, tai lähettää nimikyselyn eteenpäin toiselle nimipalvelimelle. Jos käyttäjä on kotiverkossaan ja haluaa käyttää jotain kotiverkon tarjoamista APN:stä, palautuu DNS-kyselyn tuloksena kotiverkon GGSN:n osoite. Jos käyttäjä on vieraassa verkossa ja käyttäjä haluaa käyttää tiettyjä kansainvälisesti sovittuja APN-nimiä, kuten internet, palauttaa nimipalvelin vierasverkon GGSN:n osoitteen. Jos vierasverkon nimipalvelin ei tiedä halutun APN:n osoitetta, se kysyy APN:n osoitetta muilta nimipalvelimilta. Jos vierasverkon nimipalvelin tietää käyttäjän kotiverkon nimipalvelimen osoitteen, kysytään APN:n osoitetta siltä ja muussa tapauksessa kysely ohjataan GRX-verkossa olevalle juuri-nimipalvelimelle (.gprs). GRX-verkon juuri-nimipalvelin tietää kaikkien siihen liittyneiden operaattorien nimipalvelimien osoitteet ja palauttaa kyselyiden vastauksina käyttäjien kotiverkkojen nimipalvelimien osoitteita. Kyselyn tullessa kotiverkon nimipalvelimelle, vastaa se palauttamalla kotiverkon GGSN:n osoitteen ja lähettää nimikyselyn vastauksen. Jos nimikysely tulee kotiverkkoon saakka, on kotiverkon GGSN:n tarjottava käyttäjän haluamaa APN-osoitetta, koska HLR:ssä oli määritelty, että käyttäjällä on oikeus käyttää sitä. HLR:ssä ei pitäisi olla sellaisia APN-osoitteita, joita kotiverkon GGSN ei tarjoa. Lopulta prosessin aloittaneelle SGSN:lle palautuu käytettävän GGSN:n osoite ja SGSN kytkee käyttäjän haluttuun palveluun muodostamalla GTP-tunnelin SGSN:n ja GGSN:n välille. [10][11]

Teoriassa GPRS-käyttäjät voisivat käyttää verkkovierailutilanteissa paikallisen operaattorin APN-osoitteita, mutta operaattorit eivät ole halunneet tarjota tätä ominaisuutta käyttäjilleen. Vieraan operaattorin APN:n käyttö saattaisi vaatia

asiakkaalta päätelaitteen asetusten muuttamista, mikä tekisi palveluiden käytön vieraassa verkossa asiakkaan kannalta hankalammaksi. Vieraan verkon APN-osoitteiden käyttäminen voisi aiheuttaa laskutusongelmia ja asiakkaan kokeman palvelunlaadun alenemista ilmenevien ongelmien vuoksi. Nykytilanteessa käytettäessä GPRS-palveluita vieraissa verkoissa, kaikki GPRS-liikenne ohjataan käyttäjän kotiverkon APN-osoitteisiin ja siten liikenne kulkee kotiverkon GGSN:n kautta haluttuihin palveluihin. Ohjaamalla kaikki liikenne käyttäjän kotiverkkoon, voi operaattori tarjota asiakkailleen samoja palveluita sekä kotiverkossa, että vieraissa verkoissa.

2.2 Enhanced Data for GSM Evolution (EDGE)

EDGE:n avulla operaattorit voivat tarjota GPRS-kykyisillä verkoilla suurempia siirtonopeuksia, kuin mitä GPRS-tekniikalla voidaan tarjota. EDGE:n käyttöönotto ei vaadi muutoksia GPRS-runkoverkkoon, eikä uusia taajuusalueita tarvita [11]. EDGE-toiminnallisuudet voidaan ottaa käyttöön päivittämällä olemassa olevan GSM-verkon tukiasemia ja niiden ohjelmistoja. EDGE toimii samalla taajuusalueella, kuin nykyiset GSM-verkot [12]. Päivittämällä matkapuhelinverkot ja tukiasemat EDGE-kykyisiksi, operaattoreilla olisi mahdollisuus tarjota 3G-palveluita (3rd Generation) jo ennen 3G-verkkojen valmistumista. EDGE:n käyttö vaatii sitä tukevan päätelaitteen, joten EDGE:n käyttöönotto vaatii asiakkailta uusien päätelaitteiden hankkimista. Näistä syistä EDGE voi olla operaattoreiden kannalta kiinnostava vaihtoehto suunniteltaessa verkon päivittämistä.

EDGE on kehittyneempi modulaatio GSM-tekniikasta. Se on suunniteltu välittämään dataliikennettä nopeimmillaan 384 kb/s:n nopeudella. Käytännössä EDGE:n tarjoamat siirtonopeudet eivät yllä suunniteltuun arvoon, mutta on kuitenkin 3-4-kertainen verrattuna GPRS-yhteyteen. EDGE-standardi perustuu GSM-standardiin ja käyttää samaa TDMA-kehysrakennetta (Time-Division Multiple Access) ja olemassa olevia soluja. EDGE mahdollistaa 3G-palveluiden ja sovellusten, kuten videopuheluiden, web-surffailun ja äänen ja kuvan suoratoiston [12]. Uusien 3G-palveluiden lisäksi EDGE:n

tarjoama suurempi läpäisykyky mahdollistaa myös yritysverkkojen mobiiliyhteyksien tehokkaamman käytön. EDGE:n myötä on mahdollista tarjota mobiiliverkoissa kiinteän puhelinverkon tilaajaliityntätekniikoita vastaavia tiedonsiirtoratkaisuja. EDGE:n avulla pakettikytkentäiset matkapuhelinverkot tulevat olemaan entistä kilpailukykyisempi vaihtoehto langattoman tiedonsiirron toteutuksessa.

EDGE on määritelty siten, että sillä voidaan parantaa aikavälikohtaista läpäisyä käytettäessä sekä HSCSD-, että GPRS-tekniikoita. Datanopeuksien kolminkertaistamiseen päästään käyttämällä 8-PSK (Octagonal Phase Shift Keying) modulaatiota, jota käyttämällä voidaan radiotiellä välittää yhdellä symbolilla kolme bittiä. GSM-tekniikassa käytetään GMSK-modulaatiota, (Gaussian Minimum Shift Keying) jossa yhdellä symbolilla välitetään vain yksi bitti. Tehokkaamman modulaation käyttö kasvattaa suurinta mahdollista siirtonopeutta, mutta samalla se heikentää signaalin virheensietokykyä. Heikko virheensietokyky johtaa siihen, että suurimpia siirtonopeuksia saavutetaan ainoastaan tukiasemien läheisyydessä ja suurin mahdollinen siirtonopeus laskee etäisyyden kasvaessa. Suurin hyöty EDGE:stä saadaan siis rajatuilla alueilla. [13]

2.3 Universal Mobile Telecommunications System (UMTS)

Kolmannen sukupolven matkapuhelinverkkojen perimmäinen tarkoitus oli muodostaa maailmanlaajuinen infrastruktuuri, joka kykenee välittämään nykyisiä ja tulevia mobiilipalveluita. Tähän laajaan tavoitteeseen voidaan päästä eriyttämällä liityntätekniikat, siirtotekniikat, palveluiden luontitekniikat ja käyttäjäsovellukset toisistaan. [9]

UMTS-arkkitehtuuri koostuu kolmesta yhdessä toimivasta osasta; runkoverkko, UMTS-radioverkko (UTRAN, UMTS Terrestrial Radio Access Network) ja päätelaitteet. Runkoverkon päätehtävänä on tarjota käyttäjien liikenteen kytkentää, reititystä ja

välitystä. Näiden toimintojen lisäksi runkoverkko sisältää tietokantoja ja verkonhallinta-funktioita. [14]

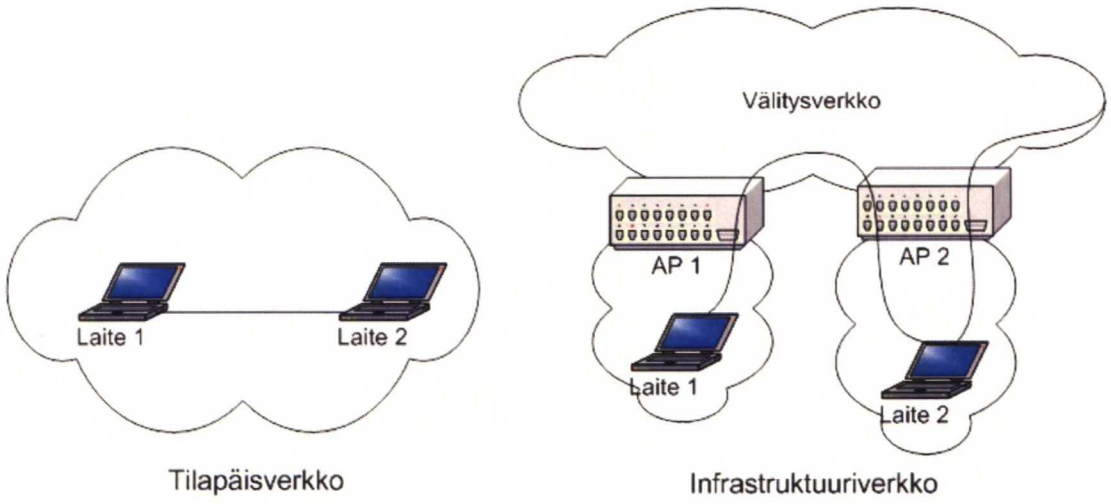
UMTS release 4 arkkitehtuurissa sekä radioverkko että runkoverkko on jaettu käsitteellisesti kahteen osaan. Radioverkko koostuu GERAN- (GPRS/EDGE Radio Access Network) ja UTRAN-radioverkoista. GERAN-radioverkko toimii toisen sukupolven päätelaitteiden radioverkkona palvellen GSM-, GPRS- ja EDGE-päätelaitteita. Tämän radioverkon rakenteellisia osia ovat tukiasemat (BTS, Base Transceiver Station) ja tukiasemaohjain (BSC, Base Station Controller). UTRAN-radioverkon osia ovat tukiasemat (BS, Base Station) ja radioverkko-ohjaimet (RNC, Radio Network Controller). [9]

UMTS release 4 arkkitehtuurissa runkoverkko on jaettu kahteen alueeseen; piirikytkentäiseen alueeseen ja pakettikytkentäiseen alueeseen. Piirikytkentäinen alue sisältää verkon reunalla olevat mediayhdyskäytävät (MGW, Media Gateway) ja matkapuhelinkeskuspalvelimen (MSC Server, Mobile Switching Centre Server). Pakettikytkentäisenä alueena toimii kappaleessa 2.1 esitelty pakettikytkentäinen GPRS-runkoverkko. Evoluution jatkuessa UMTS release 5:n runkoverkkoon tulee lisää muutoksia, joiden tarkoituksena on parantaa runkoverkon toimintaa. Release 5 myötä tulevien muutosten on tarkoitus olla käyttäjille täysin näkymättömiä. [9]

Käyttäjien näkökulmasta UMTS tarjoaa rajatuilla alueilla toimivat mobiiliyhteydet, joissa saavutettu kaistanleveys on GPRS-yhteyksien kaistaleveyttä suurempi. UMTS- ja GPRS-radioverkkojen välinen verkkovierailu mahdollistaa jatkuvien yhteyksien ylläpitämisen myös liikkuvien käyttäjien kohdalla. Käyttäjien liikkuessa UMTS-verkon toiminta-alueelta pois, siirtyy päätelaite automaattisesti käyttämään GPRS-verkkoa. Siirto verkosta toiseen on käyttäjän kannalta läpinäkyvä, eli muodostetut yhteydet säilyvät ja ainoastaan tiedonsiirtonopeus laskee.

3 LANGATTOMAT LÄHIVERKOT

Langattomilla lähiverkoilla (WLAN, Wireless Local Area Network) tarkoitetaan IEEE:n (Institute of Electrical & Electronics Engineering) määrittelemään 802.11-standardiin perustuvia verkkoja, jotka välittävät dataliikennettä ilmarajapinnan yli sähkömagneettisina aaltoina. IEEE on määritellyt 802.3-standardin (ethernet), joka on hallitseva tekniikka fyysisiin siirtojohtimiin perustuvissa lähiverkoissa (LAN, Local Area Network). WLAN-tekniikasta on vastaavasti muodostunut vastaavasti hallitseva tekniikka langattomien verkkojen alueella.



Kuva 2 Tilapäis- ja infrastruktuuriverkot

WLAN-tekniikalla voidaan muodostaa kahden tyyppisiä verkkoja; tilapäisverkkoja (ad hoc) ja infrastruktuuriverkkoja. Tilapäisverkot koostuvat yksittäisistä laitteista, jotka voivat kommunikoida ilmarajapinnan kautta ja kommunikoivat muodostamassaan verkossa keskenään. Tilapäisverkot muodostetaan tai muodostuvat tyypillisesti spontaanisti tilanteissa, joissa tietyllä alueella on kaksi tai useampia laitteita, joilla on kyky ja tarve kommunikoida keskenään. Tilapäisverkot ovat sekä ajallisesti että paikan suhteen rajattuja. Tilapäisverkko on siis olemassa ainoastaan rajallisen ajan ja toimii ainoastaan rajatulla alueella. [15] Kuvassa 3 on esitetty kaksi laitetta sekä tilapäisverkossa että infrastruktuuriverkossa. Kuten kuvasta 3 voidaan nähdä, voi kahden

laitteen muodostamassa tilapäisverkossa olla yhteys ainoastaan näiden kahden laitteen välillä. Laitteiden lisääntyessä, voidaan tilapäisverkoissa muodostaa monimutkaisempia yhteyksiä, kuten yhteys kahden laitteen välille käyttäen kolmatta laitetta välittäjänä.

Infrastruktuuriverkot koostuvat verkon liityntäpisteistä (AP, Access Point) sekä laitteista, jotka liittyvät verkkoon liityntäpisteiden kautta. Infrastruktuuriverkoissa liityntäpisteet on yhdistetty välitysverkkoon, jonka kautta on mahdollista muodostaa yhteyksiä verkon muihin osiin tai muihin verkkoihin. Kuvassa 3 on esitetty infrastruktuuriverkon rakenne, jossa välitysverkkoon on kytketty kaksi liityntäpistettä, joihin on liittynyt laitteita. Kuvassa on myös esitetty laitteiden muodostamien yhteyksien reittejä. Eri liityntäpisteisiin kytkeytyneet laitteet voivat muodostaa yhteyden yhteisen välitysverkon kautta ja muodostaa yhteyksiä ulkopuolisiin verkkoihin välitysverkon kautta. Välitysverkko voi olla joko 802.11 standardin mukainen WLAN-verkko tai muu 802-standardien mukainen LAN-verkko [15].

3.1 Langattomien lähiverkkojen standardit

Tällä hetkellä on käytössä useita vaihtoehtoisia ja toisiaan täydentäviä eri standardeihin perustuvia langattomia lähiverkkotekniikoita. IEEE määrittelee ja kehittää 802.11 standardinsa mukaisia langattomien lähiverkkojen teknologioita. 802.11b mukainen tekniikka on laajimmin käytössä oleva WLAN-tekniikka, jonka suurin mahdollinen siirtonopeus on 11 Mbps. 802.11b standardin heikkouksia ovat WLAN-verkon riittämättömät tietoturvaominaisuudet ja QoS-ominaisuuksien (Quality of Service) puuttuminen, jotka voivat vaikuttaa esimerkiksi suoratoistosovellusten käytettävyyteen. Valmistumassa oleva 802.11i-standardi tuo langattomiin lähiverkkoihin kaivattuja tietoturvaominaisuuksia, joiden avulla niiden turvallisuutta voidaan parantaa. [16] Taulukossa 1 on esitetty langattomien lähiverkkojen eri standardit ja niiden keskeisimmät ominaisuudet.

Taulukko 1 Langattomien lähiverkkojen standardit [17]

Standardi	Suurin mahdollinen siirtonopeus	Taajuus	Muuta
802.11a	54 Mbps	5 GHz	Tulossa USA:n markkinoille 2003
802.11b	11 Mbps	2,4 GHz	Laajimmin käytetty tekniikka
802.11e	QoS-palvelut WLAN-tekniikoihin		
802.11g	54 Mbps	2,4 GHz	Yhteensopiva 802.11b:n kanssa
802.11h	Eurooppalaisten säädösten mukainen 5GHz tekniikka		
802.11i	Lisäys a- ja b-standardeihin, jonka tarkoitus on parantaa näiden tekniikoiden tietoturvaa. Määrittelee uudet salausprotokollat: TKIP ja AES. Vaatii uudet laitteistot. Valmistumassa vuonna 2003		
802.11x	Määrittelee pääsynhallinnan langattomiin lähiverkkoihin. Määrittelee EAP-autentikointiprotokollan		

3.2 Langattomien lähiverkkojen käyttötarkoitukset

Langattomat lähiverkot voidaan jakaa käyttötarpeiden ja -kohteiden mukaan erilaisiin luokkiin, jotka eroavat toisistaan toteutustapojen, käyttötarkoitusten ja vaatimusten suhteen.

Infrastruktuuriin perustuvia langattomia lähiverkkoja käytetään kiinteiden verkkojen jatkeena tarjoamaan pääsy kiinteään verkkoon. Eli langattomat lähiverkot liitetään osaksi kiinteää verkkoa, jolloin koko verkon toiminta-alue laajenee.

Langattomia lähiverkkoja voidaan käyttää laajasti erilaisissa tarkoituksissa ja erilaisten verkkojen osana. Laajakaistaisten verkkoyhteyksien yleistyttyä kuluttajamarkkinoilla, on myös langattomien lähiverkkojen käyttö lisääntynyt kodeissa. Kodeissa käytetyt langattomat lähiverkot ovat siten langallisten verkkojen jatkeita ja toimivat kodeissa pääosin verkkojohtimien korvikkeina. Kotiympäristössä käytettäviin verkkoihin liittyvät

tietoturvavaatimukset ovat yleisesti alhaisempia kuin muut, esimerkiksi yritysverkkojen tietoturvavaatimukset.

Toinen langattomien lähiverkkojen tyyppi on Hot Spot-verkot. Hot Spot-verkolla tarkoitetaan julkista palvelualuetta, jossa langatonta lähiverkkoa on mahdollista käyttää joko ilmaiseksi, tai maksua vastaan. Yleisesti Hot Spot-verkossa tarjotaan käyttäjille ainoastaan pääsy julkiseen internetiin ja sitä kautta käyttäjän haluamiin palveluihin. Hot Spot-verkkoja on rakennettu esimerkiksi hotelleihin, kahviloihin, lentoasemille ja kauppakeskuksiin ja niiden käytön uskotaan lisääntyvän lähivuosina huomattavasti. Market Vision Oy:n tutkimuksen mukaan ainoastaan 13 % tutkimuksen kohteena olleista suomalaisissa yrityksissä ja julkisessa hallinnossa yksiköistä hyödyntää Hot Spot-palveluita, mutta käytön uskotaan lisääntyvän merkittävästi vuoteen 2005 mennessä. [18] Vaikka Hot Spot-palveluiden merkitys yritysten tietoliikenneyhteyksien kannalta on tällä hetkellä pieni, niin tarpeiden ja verkkojen lukumäärän kasvaessa Hot Spot-palvelut saattavat tuoda merkittävän lisän yritysten työntekijöiden tietoliikenneyhteyksiin.

Kolmas ja yritysten kannalta merkittävin langattomien lähiverkkojen tyyppi on yritysten omat langattomat lähiverkot, jotka ovat osa yritysten sisäverkkoa, tai joiden pääasiallinen tarkoitus on tarjota työntekijöille yhteys yrityksen sisäverkkoon. Langattomia lähiverkkoja hyödynnetään yleisimmin toimistoissa ja noin kolmannes Market Visionin tutkimukseen osallistuneista yrityksistä käyttää langattomia lähiverkkoja varastoissa. [18] Yrityksillä on useita eri tapoja hankkia langattomia lähiverkkoja käyttöönsä. Yrityksen kannalta vaivattomin tapa on hankkia langaton lähiverkko palveluna, jolloin palveluntarjoaja toimittaa ja asentaa verkon ja vastaa verkon ylläpidosta. Langaton lähiverkko voidaan myös rakentaa itse ostamalla tarvittavat verkkolaitteet ja ohjelmistot ja asentamalla verkko ja ohjelmistot itse. Nämä kaksi tapaa hankkia langaton lähiverkko ovat ääriesimerkkejä, joiden välille jää monia eri malleja langattomien lähiverkkojen rakentamiseen ja hallinnointiin.

4 TIETOTURVAMEKANISMIT YRITYSVERKOISSA

Tässä kappaleessa käsitellään yritysverkkojen ja yritysverkkojen mobiiliyhteyksien kannalta tärkeitä mekanismeja ja tietoturvaominaisuuksia. Kappaleessa esitellään AAA-arkkitehtuuri (Authentication, Authorization and Accounting) ja siihen perustuva RADIUS-protokolla. Lisäksi kappaleessa käsitellään pakettikytkentäisten matkapuhelinverkkojen ja langattomien lähiverkkojen tietoturvaa.

4.1 Tunnistaminen, valtuutus ja vastuunalaisuus, AAA-arkkitehtuuri

Tunnistaminen on prosessi, jossa henkilön tai laitteen ilmoittaman identiteetin oikeellisuus varmistetaan. Tunnistamismenetelmiä on lukuisa ja ne voidaan jaotella kolmeen ryhmään niiden toimintaperiaatteen mukaan.

- Tunnistamien voi perustua johonkin tietoon, joka käyttäjällä on, eli esimerkiksi salasanaan
- Tunnistaminen voi perustua johonkin mitä käyttäjä pitää hallussaan, eli esimerkiksi älykorttiin
- Tunnistaminen voi perustua johonkin mitä käyttäjä on tai osaa, kuten sormenjälkeen tai käsialaan. [19]

Yleisimmin käytetään käyttäjätunnukseen ja salasanaan perustuvia tunnistamismenetelmiä, mutta älykorttien ja biometrisen tunnistamisen yleistyminen saattaa lisätä niiden käyttöä tulevaisuudessa [19]. Tunnistuksessa tunnistettavaa identiteettiä ja tunnistusmenetelmän mukaista tietoa verrataan tunnistavan tahon tietoihin ja jos ne vastaavat toisiaan, on tunnistaminen suoritettu onnistuneesti.

Valtuutuksella tarkoitetaan käyttäjän toimenpiteiden hallitsemista, eli mitä toimenpiteitä käyttäjä saa suorittaa. Valtuutus perustuu useimmiten tunnistamisesta saatuihin tietoihin,

joiden perusteella saadaan selville mitä toimenpiteitä kukin käyttäjä saa tehdä. Valtuutuksella voidaan hallita käyttäjien pääsyä salattuihin tietoihin tai käyttäjien mahdollisuuksia käyttää tiettyjä sovelluksia tai palveluita. [19]

Tunnistamien ja valtuutus ovat usein osa yhtä prosessia, jossa käyttäjä tunnistetaan ja käyttäjälle annetaan valtuudet suorittaa tiettyjä toimintoja. Esimerkki tunnistamisesta ja valtuutuksesta on käyttäjän kirjautumien tietokoneelle. Käyttäjä syöttää käyttäjätunnuksensa ja tunnistamismekanismin mukaisen tunnisteen, esimerkiksi salasanan. Näiden tietojen avulle järjestelmä pystyy tunnistamaan käyttäjän, jonka jälkeen siirrytään valtuutukseen, eli käyttäjälle annetaan oikeutus käyttää tietokoneen resursseja valtuuksiensa mukaisesti. Jos käyttäjää ei tunnisteta, ei edetä valtuutukseen, jolloin käyttäjä ei saa oikeuksia suorittaa operaatioita. Itse tunnistaminen ei siis vielä oikeuta käyttäjää tekemään mitään, koska siinä ainoastaan selvitetään käyttäjän identiteetti. Onnistunutta tunnistusta seuraavassa valtuutuksessa hyödynnetään tunnistuksessa saatuja tietoja ja sallitaan käyttäjän haluaman tietokoneen tai sovelluksen käyttö.

Vastuunalaistaminen tarkoittaa prosessia, jossa kerätään tietoja resurssien käytöstä. Näitä tietoja voidaan käyttää esimerkiksi resurssien käytön analysointiin, laskutukseen tai palveluiden kehitystä varten [20]. Kerättyjä tietoja voidaan käyttää myös muihin tarkoituksiin, kuten jälkitarkastuksiin tai ongelmatilanteiden selvittämiseen.

Tunnistus, valtuutus ja vastuunanalaistaminen muodostavat yhdessä IETF:n määrittelemän AAA-arkkitehtuurin, jonka mukaan voidaan määritellä tietoturvaprotokollia ja palveluita [21].

RADIUS-protokolla on laajassa käytössä oleva AAA-arkkitehtuurin mukainen protokolla. RADIUS-protokolla perustuu palvelin-asiakas-malliin, jossa verkon pääsynhallintapalvelin (NAS, Network Access Server) toimii RADIUS-asiakkaana. NAS välittää kirjautuvan käyttäjän tietoja valitulle RADIUS-palvelimelle ja saatuaan vasteen, toimii sen mukaan [22]. RADIUS-arkkitehtuurin tarkoituksena on muodostaa

keskitetty tietokanta käyttäjien tiedoista, joka mahdollistaa käyttäjien tunnistamisen ja tämän lisäksi asetustietojen ja tiedon tarjolla olevista verkkopalveluista välittämisen käyttäjille [22]. RADIUS-palvelimen tehtävänä on vastaanottaa käyttäjien yhteydenmuodostuspyyntöjä, tunnistaa käyttäjät ja välittää RADIUS-asiakkaalle mahdolliset asetustiedot, joiden avulla se voi tarjota kirjautuvalle käyttäjälle pyydettyä palvelua. Arkkitehtuuri mahdollistaa myös RADIUS-palvelimien toimimisen välittäjäpalvelimina muille RADIUS-palvelimille.

RADIUS-palvelimet voivat tukea monia käyttäjän tunnistamismenetelmiä, kuten Point-to-Point protokollia tai heräte-vaste-mekanismia [22]. Kun mobiili käyttäjä haluaa kirjautua tiettyyn järjestelmään käyttäen RADIUS:ta, se esittää NAS:lle kirjautumistietoja, esimerkiksi käyttäjätunnuksen ja salasanan. NAS toimii tämän jälkeen RADIUS-asiakkaan ja välittää kirjautumispyynnön RADIUS-palvelimelle, joka varmistaa, onko NAS palvelimen tuntema käypä RADIUS-asiakas. Jos käytetään haaste-vaste-menetelmää, RADIUS-palvelin lähettää kirjautumispyynnön lähettäneelle päätelaitteelle haasteen, johon käyttäjä vastaa haasteen perusteella laskemallaan vasteella. RADIUS-palvelin lähettää RADIUS-asiakkaalle joko kirjautumisen hylkäys- tai hyväksymisviestin, ja sen mukana mahdolliset asetustiedot.

Uudistuvien ja monimutkaistuvien verkkoteknologioiden myötä myös AAA-protokollille asetettavat vaatimukset ovat kasvaneet ja IETF:n (Internet Engineering Task Force) AAA-työryhmä valmistelee uutta DIAMETER-protokollaa, joka tulee korvaamaan RADIUS-protokollan. DIAMETER:n tarkoituksena on tarjota AAA-arkkitehtuurin mukaisia palveluita sovelluksille, jotka toteuttavat pääsynhallintaa ja IP-liikkuvuutta [23]. DIAMETER-protokolla perustuu vertaisarkkitehtuuriin, jossa muodostetaan useita yhteyksiä asiakkaan, välittäjäsolmujen ja palvelimen välille, joiden kautta lähetetty pyyntö välitetään haluttuun päätepisteeseen. DIAMETER:n uusia ominaisuuksia ovat esimerkiksi palvelimen aloittamat yhteydet, virhetilanteiden hallinta, pakettien uudelleen lähetys, kuljetuskerroksen turvallisuus ja IPsec-protokollan (Internet Protocol Security) pakollisuus. DIAMETER on yhteensopiva RADIUS-protokollan

kanssa, joten käytössä olevia AAA-arkkitehtuurin mukaisia palvelimia voidaan päivittää tarpeiden mukaan.

RADIUS-autentikointia voidaan käyttää GPRS-verkon asiakkaiden tunnistamiseen. Käyttäjien tunnistus tapahtuu yhteydenmuodostusvaiheessa, kun käyttäjä on valinnut APN-osoitteen, johon yhteys muodostetaan. Jos tiettyyn APN-osoitteeseen kytkeytyvät käyttäjät tunnistetaan yksilöllisesti, on niille käyttäjille mahdollista tarjota yksilöllisiä käyttäjä- tai käyttäjäryhmäkohtaisia palveluita. Käyttämällä RADIUS-protokollaa, voidaan käyttäjän MSISDN-numeron (Mobile Subscriber ISDN Number) perusteella määrittää, mitä palveluita käyttäjälle tarjotaan, ja mitä yhteyksiä käyttäjä saa muodostaa. [11] Mikäli APN-osoitteeseen kytkeytyviä käyttäjiä ei tunnisteta, tarjotaan kaikille käyttäjille samoja palveluita. Yhdistämällä käyttäjän saama IP-osoite MSISDN- ja käyttöoikeustietoihin, voidaan lisäpalveluita tarjota IP-osoitteisiin perustuvan tunnistuksen avulla. RADIUS-arkkitehtuuri mahdollistaa tietueiden välittämisen toisille RADIUS-palvelimille, jolloin palveluntarjoajat ja operaattorin asiakkaat voivat hyödyntää IP-osoitteisiin perustuvaa tunnistusta omissa palveluissaan ja järjestelmissään.

4.2 Tietoturva pakettikytkentäisissä matkapuhelinverkoissa

Pakettikytkentäisten matkapuhelinverkkojen tietoturvaominaisuudet toimivat pääosin OSI-mallin (Open Systems Interconnection) verkkokerroksen alapuolella, tarjoten tietoturvaominaisuuksia kyseisen verkon sisällä. OSI-mallin verkkokerroksella ja sitä ylemmillä kerroksilla tarvittavat tietoturvamekanismit on toteutettava muilla, näistä verkosta riippumattomilla tekniikoilla. Tässä työssä tarkastellaan ratkaisuja, jotka toimivat pääosin OSI-mallin verkkokerroksella sekä sitä ylemmillä kerroksilla ja jotka toimivat lisäksi usean eri verkon alueella. Näissä ratkaisuissa käytettävien tietoturvaratkaisuiden on toimittava saumattomasti liikenteen kulkiessa verkkojen rajapintojen yli. Pakettikytkentäisten matkapuhelinverkkojen tietoturvaominaisuudet eivät tarjoa käsiteltävien ratkaisuiden kannalta riittävän laajoja tietoturvapalveluita.

Koska pakettikytkentäiset matkapuhelinverkot ovat kuitenkin merkittävässä asemassa käsiteltäessä tässä työssä arvioitavia ratkaisuja, käsitellään näiden verkkojen tietoturvaominaisuuksia seuraavissa kappaleissa lyhyesti.

4.2.1 Tietoturva GPRS-verkossa

GPRS-verkon tietoturvafunktioiden tarkoitus on estää luvaton GPRS-palvelun käyttö autentikoinnilla ja palvelupyyntöjen kelpuutuksella, taata käyttäjien identiteetin luottamuksellisuus väliaikaisilla identiteeteillä ja salakirjoituksella sekä taata käyttäjien datan luottamuksellisuus salakirjoituksella [8]. GSM-järjestelmässä, jonka osana GPRS-palvelu toimii, turvafunktiot keskittyvät radiotien salaukseen [9]. GSM-järjestelmän tärkeimpiä tietoturvaominaisuuksia ovat:

- Käyttäjien autentikointi
- Radiotien kommunikaation salaus
- Väliaikaisten identiteettien käyttö. [8][9]

GPRS-verkossa päätelaitteet autentikoidaan SGSN:ssä HLR:ssä olevien käyttäjätietojen avulla. SGSN käyttää autentikoinnissa haasteeseen ja vasteeseen perustuvaa autentikointimenetelmää [11]. Prosessissa SGSN generoi haasteen, joka lähetetään päätelaitteelle ja sillä olevalle SIM-kortille (Subscriber Identity Module). Päätelaite laskee haastetta vastaavan vasteen, joka lähetetään takaisin SGSN:lle.

Käyttäjien identiteetin luottamuksellisuuden takaamiseksi käytetään väliaikaisia identiteettejä ja pyritään välttämään IMSI-numeron käyttöä. Väliaikaiset identiteetit voidaan yhdistää tarvittaessa käyttäjien IMSI-numeroon jokaisessa SGSN:ssä olevien tietokantojen avulla. [11]

4.2.2 Tietoturva UMTS-verkossa

GSM-järjestelmässä tietoturvaominaisuudet keskittyvät radiotien liikenteen salaukseen, mutta UMTS-järjestelmässä tietoturva on tätä laajempi käsite. UMTS-verkon tietoturvaominaisuudet pohjautuvat GSM-järjestelmän ominaisuuksiin, mutta myös lisäyksiä ja muutoksia on tehty. [9]

UMTS-järjestelmän tärkeimpiä tietoturvaominaisuuksia ovat:

- Käyttäjän ja verkon molemminpuolinen autentikointi
- Väliaikaisten identiteettien käyttö
- Radiotien kommunikaation salaus
- Signaloinnin eheyden turvaaminen UTRAN-verkon sisällä. [9]

UMTS-järjestelmän autentikointiprosessiin osallistuu käyttäjän kotiverkko, käyttäjää palveleva verkko ja päätelaiteessa oleva USIM-älykortti (Universal Subscriber Identity Module). Autentikointiprosessissa tarkistetaan päätelaitteen identiteetin haaste-vaste menetelmällä ja päätelaite varmistaa kotiverkolta, että palveleva verkko saa suorittaa autentikoinnin. GSM-järjestelmässä tarkistettiin ainoastaan päätelaitteen identiteetti, mutta UMTS-järjestelmässä päätelaite tarkistaa palvelevan verkon oikeutuksen. [9]

Väliaikaisten identiteettien käyttö UMTS-järjestelmässä on GSM-järjestelmän kaltainen, mutta GSM-järjestelmässä käytetyn yhden väliaikaisen identiteetin tilalla UMTS:ssä käytetään kahta eri identiteettiä. UMTS-järjestelmän pakettikytkentäisessä osassa käytetään eri identiteettiä, kuin piirikytkentäisessä osassa. [9]

Signalointiliikenteen eheyden turvaamisella pyritään yksittäisten hallintaviestien autentikoitavuuteen. Tämä menettely on tärkeä, koska kahden välinen autentikointi varmistaa kommunikoivien tahojen identiteetit ainoastaan autentikointihetkellä.

Autentikointiprosessin jälkeen man-in-the-middle hyökkäys olisi mahdollinen, jos jokaista hallintaviestiä ei autentikoitaisi. [9]

UMTS release 5 myötä järjestelmän runkoverkko on mahdollista toteuttaa kokonaan IP-protokollaan perustuvana, jolloin siihen kohdistuvat kaikki IP-protokollan tietoturvauhat. IP-protokollan suojaamiseen on olemassa olevia keinoja, kuten IPsec-protokolla, jota voidaan käyttää myös UMTS-järjestelmässä.

4.3 Langattomien lähiverkkojen tietoturva

Kuten kaikissa tietoliikenneratkaisuissa, myös langattomien verkkojen tietoturvan tasoa on tärkeä arvioida. Langattomaan lähiverkkoon voi liittyä tukiasemien kattaman alueen sisältä riippumatta liittyvän päätelaitteen sijainnista, jolloin verkkoa voidaan käyttää myös pääasiallisen käyttöalueen ulkopuolelta, kuten yrityksen toimitilojen välittömästä läheisyydestä tai viereisen yrityksen tiloista. Tukiasemien muodostamaan verkon peittoalueeseen on kiinnitettävä huomiota, mutta sen tarkka rajaaminen ei silti riitä, koska luvattomat käyttäjät saattavat päästä langattoman verkon alueelle luvallisesti. Langattomia lähiverkkoja käytetään myös yleisillä paikoilla kuten lentokentillä ja paikoissa, joissa tarjotaan Hot Spot-palvelua.

Käytettäessä langattomia lähiverkkoja on oletettava, että verkkoon pääsyä ei voida riittävästi hallita fyysisillä ratkaisuilla, vaan pääsynhallinnassa on käytettävä muita hallintamenetelmiä. Langattomien lähiverkkojen suojauksessa käytetään edelleen WEP-salausta (Wired Equivalent Privacy), joka perustuu jaettuun salaisuuteen ja korkeintaan 128-bittisiin avaimiin, mutta se ei tarjoa riittävää suojaa mahdollisia hyökkäyksiä vastaan [24]. WEP-salauksen avaimet on mahdollista murtaa esimerkiksi Airsnort- tai WEPCrack-ohjelmilla, jotka ovat vapaasti saatavilla Internetistä, eikä niiden käyttö vaadi teknistä osaamista. Murtamalla WEP-salauksen tunkeutuja pääsee käyttämään verkkoa huomiota herättämättä ja murtamiseen kuluu aikaa ainoastaan muutamia tunteja riippuen verkossa välitettävän liikenteen määrästä. [25][26]

Langattomien lähiverkkojen tietoturvan parantamiseksi on useita eri vaihtoehtoja, joista esittelen lyhyesti IEEE:n standardoimat 802.1x- ja 802.11i-tekniikat ja VPN-tekniikoiden (Virtual Private Network) käytön langattomassa lähiverkkoympäristössä.

IEEE 802.1x on standardoitu menetelmä, jolla voidaan autentikoida verkkoon kirjautuvat laitteet. 802.1x-standardi määrittelee arkkitehtuuriratkaisun, joka sisältää verkkoon kytkeytyvän päätelaitteen, autentikoijan, autentikoitipalvelimen ja verkon, johon käyttäjä on kytkeytymässä. Autentikoija on käyttäjän ja verkon rajapinnassa oleva kytkin, joka hallitsee porttien tiloja joko sallimalla portin kautta kulkevan liikenteen tai estävän sen. Autentikointipalvelimena toimii standardin mukainen RADIUS-palvelin.

802.1x-stadardi käyttää IETF:n määrittelemää RADIUS-protokollaa, EAP-standardeja (PPP Extensible Authentication Protocol) sekä RADIUS-protokollaan määriteltyjä laajennuksia (RFC 2284, 2865, 2869) [27]. EAP-protokollan eri versiot mahdollistavat useiden eri autentikointimenetelmien käytön, kuten SIM-kortteihin pohjautuvan tunnistuksen. IEEE 802.1x-stadardin mukaisessa ratkaisussa verkkoon kytkeytyvä laite lähettää EAP-protokollaa käyttäen autentikointiviestin autentikoijalle, joka välittää viestin autentikointipalvelimelle. Autentikointipalvelin joko hylkää tai hyväksyy pyynnön. Jos autentikointipyyntö hyväksytään, sallii autentikoija kyseisen käyttäjän käyttämän portin kautta kulkevan liikenteen, jolloin käyttäjän liikenne välitetään haluttuun verkkoon.

IEEE on määrittelemässä uutta 802.11i-standardia, joka perustuu 802.1x määritelmään ja tämän uuden standardin tarkoituksena on parantaa 802.11a- ja 802.11b-standardien mukaisten langattomien lähiverkkojen tietoturvaa. 802.11i-standardissa määritellään uusia salausavainprotokollia, kuten TKIP (Temporal Key Integrity Protocol) ja AES (Advanced Encryption Standard). TKIP on uusi versio langattomien lähiverkkojen salauksessa käytetystä WEP-protokollasta, jossa on korjattu WEP-protokollassa havaittuja ongelmia. AES on Yhdysvaltojen hallituksen toimesta kehitettävä uusi kryptografinen algoritmi, jonka on tarkoitus korvata aiemmin käytössä olleet DES (Data

Encryption Standard) ja 3DES-algortimit (Triple Data Encryption Standard). [28] 802.11i-standardin käyttöönotto vaatii laitekannan uusimisen, joten sen yleistyminen tulee olemaan hidasta. Toistaiseksi langattomien lähiverkkojen käyttäjien on siis tyydyttävä olemassa oleviin ratkaisuihin ja luotava turvalliset yhteydet esimerkiksi VPN-ratkaisuja käyttämällä.

Käytettäessä langattomia lähiverkkoja yritysverkkojen osana ei välttämättä haluta luottaa pelkkään langattoman lähiverkon tarjoamaan tietoturvaan. Tällöin langatonta lähiverkkoa käsitellään yrityksen verkosta täysin ulkopuolisena verkkona, jonka yhteydessä vaaditaan käytettäväksi muita tietoturvamekanismeja. Käsiteltäessä langatonta lähiverkkoa ulkopuolisena verkkona, voidaan sitä tarjota myös yrityksen ulkopuolisille käyttäjille; kuten yrityksen vieraina oleville yrityksen ulkopuolisille henkilöille. Yrityksen omat työntekijät voivat käyttää langatonta lähiverkkoa kuten mitä tahansa ulkopuolista langatonta tai kiinteää verkkoa, joiden kautta muodostetaan yhteys yrityksen sisäverkkoon. Yhteyden muodostamiseen turvattomasta langattomasta lähiverkosta voidaan käyttää asiakas-palvelin malliin perustuvaa VPN-ratkaisua. Tässä ratkaisussa käyttäjä muodostaa langattoman lähiverkon kautta yhteyden yrityksen suojatun sisäverkon reunalla sijaitsevaan VPN-yhdyskäytävään, jonka kautta käyttäjä yhdistetään yrityksen tietoverkkoon.

VPN-ratkaisua voidaan käyttää yrityksen omassakin lähiverkossa, jos halutaan taata muita mobiiliverkkoja vastaava tietoturvan taso. Käyttämällä asiakas-palvelin mallin mukaista VPN-ratkaisua voidaan verkkoa tarjota yrityksen työntekijöille ja silti estää mahdollinen luvaton käyttö. Tällöin langaton lähiverkko rakennetaan siten, että kaikki siitä muodostettavat yhteyden muodostetaan yrityksen VPN-yhdyskäytävään, jossa käyttäjät autentikoidaan. Tällöin yrityksen työntekijät muodostavat yhteyden yrityksen sisäiseen verkkoon ja luvattomat käyttäjät eivät voi hyödyntää langatonta lähiverkkoa, koska kaikki liikenne ohjataan VPN-palvelimelle, joka ei välitä autentikoimattomien käyttäjien liikennettä eteenpäin.

4.3.1 Julkisten langattomien lähiverkkojen aiheuttamat uhat

Vaikka langattomien lähiverkkojen kautta muodostettavissa yhteyksissä käytettäisiin VPN-ratkaisua, kohdistuu käytettävään päätelaitteeseen silti tietoturvauhkia, jotka tulee ottaa huomioon suunniteltaessa langattomien lähiverkkojen käyttöä.

- Langattomaan lähiverkkoon kytkeytyneiden päätelaitteiden jaetut levyosiot ovat näkyvissä muille saman verkon käyttäjille
- VPN-yhteyden ohi lähetettävän liikenteen salakuuntelu tai kaappaus
- Puskureiden ylivuotohyökkäykset. [29]

Windows-käyttöjärjestelmä mahdollistaa kiintolevyn osioiden jakamisen verkossa. Levyjaoissa voidaan käyttää eri tietoturvan tasoja, mutta oletuksena jaettuun levyyn asetetaan täydet oikeudet kaikille käyttäjille [29]. Levyjakoja käytetään yleisesti yritysten sisäisissä lähiverkoissa, mutta tehdyt levyjaot toimivat, vaikka tietokone siirtyy yritysverkon ulkopuolelle. Windows-käyttöjärjestelmä mahdollistaa levyjakojen etsimisen saman aliverkon alueelta, jolloin Hot Spot-verkossa olevien päätelaitteiden suojaamattomat levyjaot ovat kaikkien saman verkon käyttäjien ulottuville. Tämän ominaisuuden takia kovalevyjen jaetuilla osilla olevien suojaamattomien tietojen luottamuksellisuus vaarantuu. Windows-käyttöjärjestelmän levyjako aiheuttaa siis suuren riskin käytettäessä päätelaitteita Hot Spot-verkoissa.

Joissain VPN-ratkaisuissa on mahdollista vähentää VPN-yhteyden kuormitusta ohjaamalla yksityisverkon ulkopuolelle menevä liikenne suoraan liityntäverkon kautta Internetiin. Tällaisen VPN-ratkaisun käytöstä voidaan käyttää termiä osittainen VPN. Käytettäessä osittaista VPN-yhteyttä julkisessa langattomassa lähiverkossa on mahdollista, että liikennettä salakuunnellaan tai kaapataan. Vaikka yrityksen verkkopalveluihin liittyvä liikenne ohjataan VPN-tunneliin, saattaa julkiseen verkkoon ohjattava liikenne sisältää salaista tietoa, kuten internetpalveluiden salasanoja, joita mahdollinen salakuuntelija voi käyttää hyväkseen.

Puskureiden ylivuotohyökkäykset eivät ole pelkästään langattomissa lähiverkoissa käytetty hyökkäys, joten en esittele hyökkäystä erityisesti. Langattomissa lähiverkoissa samassa aliverkossa olevilla laitteilla on vapaat yhteyden muiden laitteiden kaikkiin portteihin ja niitä voidaan hyödyntää ylivuotohyökkäystä tehtäessä [29]. Ylivuotohyökkäykset kohdistuvat toisessa tietokoneessa olevaan ohjelmaan, joka saadaan toimimaan hyökkääjän tahtomalla tavalla aiheuttamalla ohjelmaan virhetilanne.

4.3.2 Langattomat lähiverkot kodeissa

Langattomat lähiverkot ovat yleistymässä myös kodeissa, joissa langaton lähiverkko rakennetaan usein laajakaistayhteyden jatkeeksi mahdollistamaan langattomien päätelaitteiden käyttö kodin alueella. Yritysten näkökulmasta tämä trendi saattaa vaikuttaa yritysverkkojen tietoturvaan, jos työntekijät liittävät työntekoon liittyviä laitteita kotona olevaan langattomaan lähiverkkoon.

Kotiin asennetussa langattomassa lähiverkossa saatetaan käyttää tietoturvan tasoltaan liian alhaisia suojausmenetelmiä ja yrityksen on hankala valvoa työntekijöiden kodeissa olevien verkkojen tietoturvan tasoa. Työntekijöitä voidaan ohjeistaa langattomien lähiverkkojen käytöstä, mutta yrityksen tietohallinnolla ei ole mahdollisuuksia valvoa tai hallinnoida työntekijöiden kodeissaan käyttämiä langattomia lähiverkkoja.

Kotona käytetyistä langattomista lähiverkoista aiheutuu kahdenlaisia tietoturvariskejä yritykselle. Yritysten työntekijät voivat tehdä etätyötä kodeistaan, jolloin työntekijät tarvitsevat yhteyksiä yrityksen tietoverkkoon. Muodostettaessa yhteys yrityksen tietoverkkoon kodissa olevasta langattomasta lähiverkosta, on mahdollista että langatonta lähiverkkoa luvattomasti käyttävät henkilöt voivat muodostaa yhteyksiä yrityksen tietoverkkoon työntekijän käyttämän päätelaitteen kautta tai sitä hyväksikäyttäen.

Vaikka yrityksen työntekijät eivät muodostaisi yhteyksiä kodeissa olevista langattomista lähiverkoista yrityksen tietoverkkoon, aiheutuu yrityksen päätelaitteiden liittämisestä

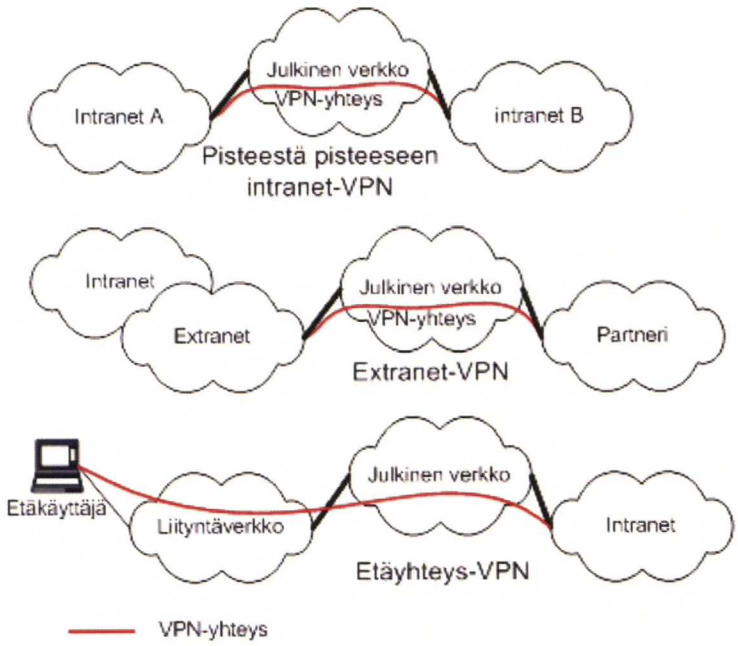
langattomaan lähiverkkoon silti tietoturvariskejä yritykselle. Jos kodeissa olevien langattomien lähiverkkojen tietoturvan taso ei ole riittävä, on mahdollista, että luvattomat käyttäjät pääsevät käyttämään niitä verkkoja. Työntekijän liittäessä yrityksen päätelaitteen kotona olevaan langattomaan lähiverkkoon, on mahdollista, että luvattomat käyttäjät pääsevät käsiksi päätelaitteelle oleviin luottamuksellisiin tietoihin ja tiedostoihin, jolloin niiden luottamuksellisuus vaarantuu.

5 VIRTUAALISET YKSITYISVERKOT

Erityisesti yritysten toiminta on tullut riippuvaiseksi tele- ja dataliikenteestä ja niitä välittävistä verkoista. Aikaisemmin yritysten tietoverkot ovat olleet erillisiä lähiverkkoja, mutta tietoliikenteen merkityksen kasvaessa on yrityksen eri toimipisteissä olevia verkkoja haluttu yhdistää toisiinsa. Tietoliikenneoperaattorit ovat tarjonneet yritysverkkojen yhdistämistä pääasiassa Frame Relay- ja ATM-yhteyksillä, sekä lähiaikoina Ethernet- ja IP-pohjaisilla tunneleilla. Verkkoa, joka yhdistää useita erillisiä verkkoja yhdeksi yhteiseksi, jaetuksi verkoksi kutsutaan virtuaaliseksi yksityisverkoksi (VPN, Virtual Private Network). Jos toimipisteet kuuluvat samaan organisaatioon, kutsutaan VPN-verkkoa intranetiksi ja jos yhteenliitettynä on yhteistyötä tekevien eri organisaatioiden toimipisteitä, kutsutaan verkkoa extranetiksi. [30] Virtuaaliset yksityisverkot voidaan määritellä myös hieman laajemmin, jolloin virtuaalisen yksityisverkon muodostavat verkot sekä yksittäiset laitteet, jotka on julkisten verkkojen kautta kulkevien yhteyksien avulla liitetty osaksi yhtä hallinnollista verkkoa. Tällainen verkko on yksityisverkko, koska verkkoon kuuluvat vain tietyt aliverkot ja laitteet ja verkossa käytetään pääsynhallintaa. Sama verkko on virtuaalinen yksityisverkko, koska kaikki aliverkot ja laitteet eivät ole fyysisesti samassa verkossa.

5.1 VPN-arkkitehtuurit

Yleisellä tasolla VPN-arkkitehtuurit voidaan jakaa kolmeen luokkaan: pisteestä pisteeseen intranet-VPN, extranet-VPN ja etäyhteys-VPN. [31] Kuvassa 4 on esitelty nämä kolme VPN-arkkitehtuuria.



Kuva 3 VPN-arkkitehtuurit

Pisteestä pisteeseen intranet-VPN kuvaa käyttötarkoitusta, jossa useita, maantieteellisesti erillään sijaitsevia, samaan organisaatioon kuuluvia verkkoja yhdistetään toisiinsa käyttäen VPN-ratkaisua. Erilliset verkot voivat sisältää useita aliverkkoja, jotka muodostavat yhdessä tietyn kohteen intranetin. VPN-ratkaisuja käytetään yhdistämään nämä erillään sijaitsevat verkot suuremmaksi yrityksen intranetiksi. [31] Yhdistettäessä Intranet-verkkoja VPN-yhteydellä toisiinsa, liitetään verkot Internetiin usein kiinteällä laajakaistaisella yhteydellä.

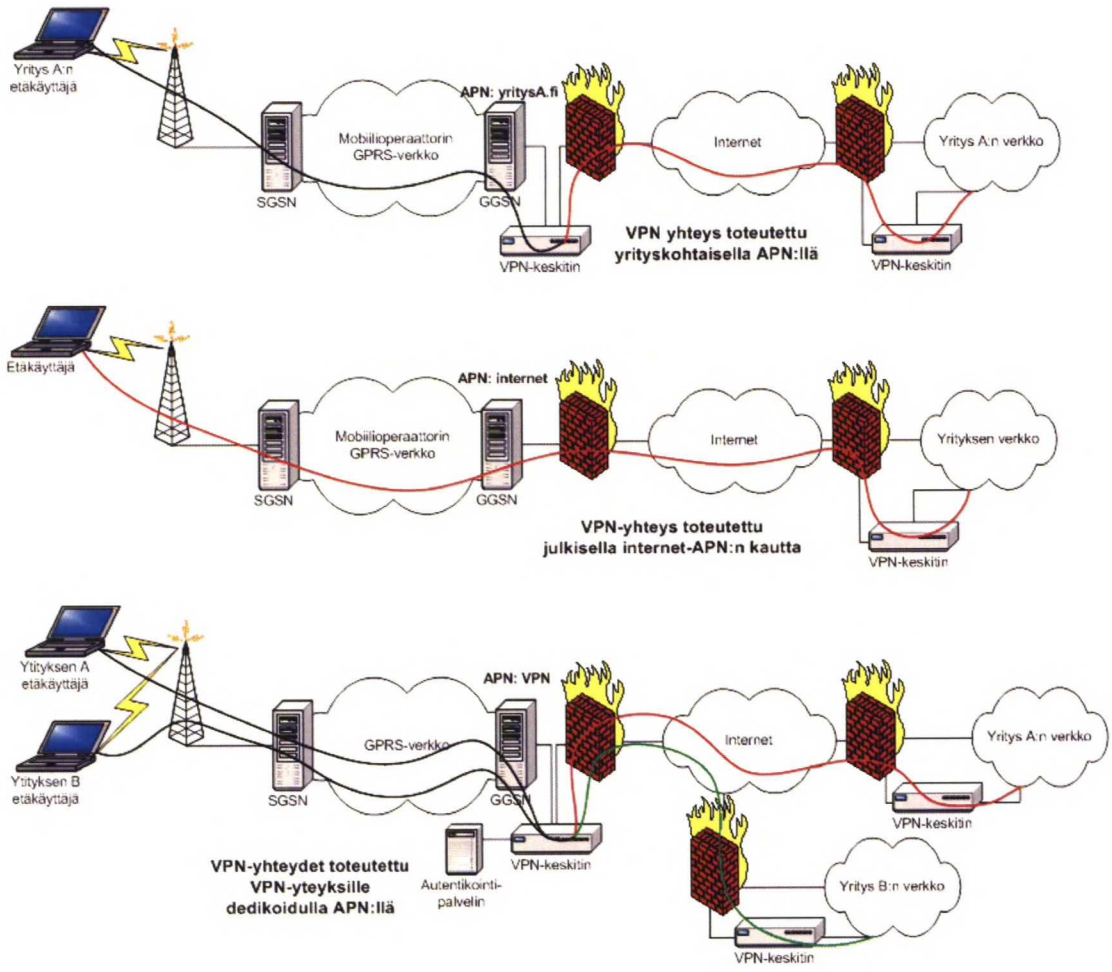
Extranet VPN-ratkaisuissa ulkopuolisille yrityksille tarjotaan pääsyä yrityksen sisäisiin verkkoihin yhteistyön tai suoritettavien transaktioiden tekemistä varten. Extranet VPN poikkeaa intranet VPN-ratkaisuista, koska se koostuu useista hallinnollista verkkoalueista ja ulkopuolisten liityntöjen käyttöön tarjotaan sisäverkon resursseja rajoitetusti. [31] Extranet VPN-ratkaisuiden tarkoitus on tarjota yrityksen partnereille pääsy rajattuun joukkoon yrityksen sisäisiä palveluita. Extranet VPN-ratkaisuissa yhteys muodostetaan kahden yrityksen kiinteiden verkkojen välille muodostamalla VPN-tunneli esimerkiksi verkkojen reunareitittimien välille. Partnerin työntekijät voivat toki käyttää

extranet VPN-palveluita mobiiliyhteyden kautta, mutta tällöin partnerin työntekijät käyttävät etäyhteys VPN-ratkaisua päästäkseen partnerin verkkoon ja extranet VPN-ratkaisua päästäkseen partnerin verkosta yrityksen extranetiin.

Etäyhteys VPN-ratkaisuja käytetään yksittäisten käyttäjien liittämiseksi yrityksen sisäiseen verkkoon sen ulkopuolelta. Yksittäinen käyttäjä voi liittyä yrityksen verkkoon lankamodeemilla, kaapelimodeemilla, käyttäen DSL-tekniikkaa (Digital Subscriber Line) tai mobiiliverkkoja. [31] Tämä työ keskittyy langattomia verkkoja käyttävien etäyhteys VPN-ratkaisuiden käsittelyyn, koska langattomia yhteyksiä käyttäen yksittäiset käyttäjät voivat olla yhteydessä yrityksen tietoverkkoon paikasta ja liikkuvuudesta riippumatta. Langattomien verkkojen käytön myötä etäyhteys VPN-ratkaisuiden käyttömahdollisuudet lisääntyvät merkittävästi luoden uusia toimintamalleja työntekijöiden työskentelyyn yrityksen toimipisteiden ulkopuolella. Langattoman tiedonsiirron kehittyminen mahdollistaa aikaisempaa tehokkaamman etäkäytön. Tähän tarvitaan VPN-ratkaisuja, joita voidaan hyödyntää mobiiliverkoissa.

5.1.1 Pakettikytkentäisten matkapuhelinverkkojen VPN-arkkitehtuurit

Pakettikytkentäisiä matkapuhelinverkkoja käyttävien etäyhteys VPN-ratkaisuiden toteuttamiseksi on kolme eri arkkitehtuurivaihtoehtoa: operaattorin julkinen internet GPRS-APN, operaattorin tarjoamille VPN-ratkaisuille dedikoitu GPRS-APN ja operaattorin tarjoama yrityskohtainen GPRS-APN. Nämä kolme eri arkkitehtuurivaihtoehtoa on esitelty kuvassa 4.



Kuva 4 Etäyhteys VPN-arkkitehtuurit mobiiliverkoissa

Operaattorin julkista Internet GPRS-APN käytettäessä käyttäjä kytkeytyy operaattorin verkkoon suojaamatonta Internet liikennettä tarjoavaan palveluun. Tämä APN ei tarjoa käyttäjälle mitään tietoturvaa Internetissä liikkuville paketeille, vaan turvallinen yhteys on muodostettava erikseen. Turvallisen yhteyden muodostamiseksi tätä palvelua käyttävillä yrityksillä on omassa verkossaan VPN-palvelin ja yrityksen verkkoon kytkeytyvillä käyttäjillä on päätelaitteissaan VPN-asiakasohjelmistot. Käyttäjä muodostaa turvallisen yhteyden yrityksen verkkoon VPN-asiakasohjelmistolla, joka salaa päätelaitteen ja yrityksen VPN-palvelimen välillä kulkevan liikenteen. Välitettävän liikenteen salauksessa voidaan käyttää esimerkiksi IPsec-protokollaa. Toteutettaessa

yrityksen VPN-ratkaisu tällä mallilla, asiakas ostaa operaattorilta pääsyn verkkoon ja voi hankkia VPN-ohjelmistot erilliseltä toimittajalta.

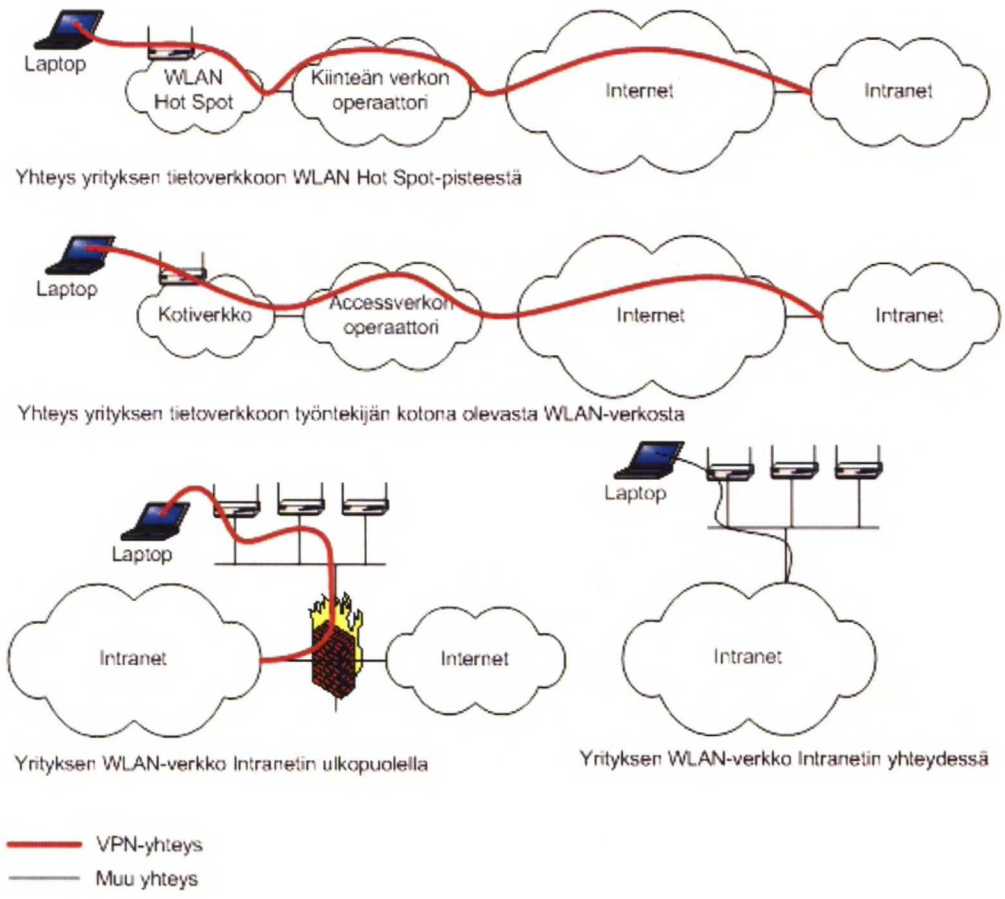
Operaattorin tarjoamassa VPN-APN-ratkaisussa käyttäjät kytkeytyvät VPN-käyttäjille dedikoituun GPRS-APN:ään, joka tunnistaa kytkeytyvän käyttäjän valituilla tunnistusmekanismeilla. Tunnistuksen jälkeen käyttäjän liikenne ohjataan kulkemaan operaattorin verkossa olevan VPN-palvelimen kautta, joka muodostaa salatun VPN-yhteyden yrityksen omaan VPN-palvelimeen. Tässä ratkaisuissa käyttäjien päätelaitteisiin ei tarvita VPN-ratkaisun käyttöä varten uutta asiakasohjelmistoa, koska salattu yhteys muodostetaan operaattorin runkoverkon ja yrityksen verkon välille. Ohjattaessa useiden yritysten käyttäjiä saman VPN-yhdyskäytävän kautta on käytettävä tunnistusmekanismeja, joiden avulla voidaan erotella eri yritysten yhteydet toisistaan. Käyttäjien tunnistamisessa voidaan käyttää RADIUS-protokollaa, jonka toiminta on kuvattu kappaleessa 4.1.. RADIUS-protokollan avulla voidaan ylläpitää tietoa käyttäjien saamista IP-osoitteista ja käyttää niitä tunnistamisessa.

Kun RADIUS-protokollaa käytetään käyttäjien tunnistamisessa mobiiliverkossa, käyttäjän MSISDN-numero liitetään käyttäjän päätelaitteen saamaan IP-osoitteeseen. Tieto IP- MSISDN-pareista tallennetaan RADIUS-palvelimelle, josta sitä kysytään tarvittaessa. RADIUS-palvelimen ilmoittamien tietojen perusteella yrityksen työntekijöiden liikenne ohjataan oikeaan VPN-tunneliin.

Käytettäessä operaattorin tarjoamaa yrityskohtaista APN:ää, reititetään kaikki kyseiseen APN:ään tuleva liikenne VPN-tunnelin läpi yrityksen omaan verkkoon. Reititettäessä käyttäjien liikenne yrityksen omaan verkkoon, voidaan käyttäjät autentikoida yrityksen omilla menetelmillä kuten, yrityksen omalla RADIUS-palvelimella. Lisäksi tämä reititystapa mahdollistaa muiden IP-verkon palveluiden kuten DHCP- ja DNS-palveluita.

5.1.2 Langattomien lähiverkkojen VPN-arkkitehtuurit

Yritysten työntekijät muodostavat yhteyksiä yrityksen tietoverkkoon langattomien lähiverkkojen kautta monilla eri tavoilla. Kuvassa 6 on esitelty neljä eri tapaa muodostaa VPN-yhteys yrityksen tietoverkkoon langattoman lähiverkon kautta. Näistä neljästä eri tavasta kolmessa käytetään VPN-yhteyttä tietoliikenteen suojaamiseen ja neljännessä tavassa tietoliikenne voidaan suojata langattomien lähiverkkojen tietoturvamekanismeilla. Myös niissä tapauksissa, joissa käytetään VPN-yhteyttä, voidaan lisäksi käyttää langattomien lähiverkkojen omia, turvallisuutta parantavia tekniikoita.



Kuva 5 Yhteydet yrityksen tietoverkkoon langattomien lähiverkkojen kautta

Hot Spot-verkot tarjoavat käyttäjilleen suojaamattomat yhteydet julkisen Internetin palveluihin. Kappaleessa 4.3.1 on esitetty Hot Spot-verkkoihin liittyviä tietoturvaongelmia. Esiteltyjen tietoturvaongelmien lisäksi Hot Spot-verkkojen käytössä tulee noudattaa suurta varovaisuutta, koska niiden toteutuksesta tai hallinasta on käyttäjällä tai käyttäjän työnantajana toimivan yrityksen tietoturvasta vastaavalla organisaatiolla ainoastaan vähän tietoa. Hot Spot-verkkoja käytettäessä tulisi aina käyttää VPN-yhteyttä, jossa kaikki liikenne välitetään yrityksen oman verkon kautta, eikä käyttää esimerkiksi osittaista VPN-ratkaisua.

Työntekijän kotona oleva langaton lähiverkko on yrityksen tietoturvan kannalta vaarallinen ympäristö, koska tietoturvasta vastaavalla organisaatiolla ei usein ole

mahdollisuutta vaikuttaa näiden verkkojen toteutukseen. Koska kotona olevat langattomat lähiverkot saattavat olla yhtä turvattomia kuin Hot Spot-verkot, tulisi niissä aina käyttää VPN-yhteyttä, kun yrityksen tietokone kytketään niihin.

Arkkitehtuuriltaan yksinkertaisin tapa toteuttaa yhteys yrityksen tietoverkkoon langattoman lähiverkon kautta on liittää verkot suoraan toisiinsa, eli kytkeä langaton lähiverkko suoraan yrityksen lähiverkkoon. Tässä toteutusvaihtoehdossa langaton lähiverkko toimii yrityksen lähiverkon langattomana jatkeena ja on sitä käyttäville työntekijöille helppokäyttöinen ja näkymätön. Käyttäjien kannalta tämä arkkitehtuuri on yksinkertainen ja verkkoa on helppo käyttää, koska käyttäjiltä ei vaadita erillistä autentikointia. Yksinkertaisuus saavutetaan tietoturvan kustannuksella, koska tässä toteutuksessa käytetään langattomien lähiverkkojen tietoturvaominaisuuksia ja tällöin on luotettava siihen tekniikkaan, jota lähiverkkojen valmistajat tarjoavat. Langattomien lähiverkkojen standardeja kehitetään jatkuvasti ja yksi niiden kehittämisen tarkoituksista on parantaa verkkojen turvallisuutta. Yhdistämällä langaton lähiverkko suoraan yrityksen sisäverkkoon, altistuu myös sisäverkko samoille tietoturvauhkille, joille langattomat lähiverkotkin altistuvat. Luvattomat käyttäjät voivat päästä käyttämään langatonta lähiverkkoa ja jos se on kiinteästi yhteydessä lähiverkkoon, on luvattomilla käyttäjillä pääsy myös lähiverkon palveluihin.

Yrityksen oma langaton lähiverkko voidaan toteuttaa myös toisella tavalla, sijoittamalla se yrityksen palomuurin ulkopuolelle verkkotopologian kannalta yrityksen lähiverkosta erilleen. Tällöin palomuurilla ja reitityksen suunnittelulla voidaan ohjata kaikki lähiverkon käyttäjät autentikoitaviksi autentikointipalvelimelle, joka joko sallii käyttäjän liikennöidä yrityksen sisäverkkoon tai estää kaiken liikenteen. Tämän arkkitehtuurin mukaisessa toteutuksessa on myös mahdollista tarjota yrityksen vieraille mahdollisuus käyttää langatonta lähiverkkoa ohjaamalla kaikki heidän liikenne langattomasta lähiverkosta suoraan julkiseen Internetiin.

5.2 Tunnelointiprotokollat

Tunnelointiteknologiat voivat perustua OSI-mallin kerrosten 2 (siirtoyhteyskerros) tai 3 (verkkokerros) protokolliin. OSI-mallin kerros 2 on siirtoyhteyskerros, joka välittää kehyksistä muodostuvaa liikennettä. L2TP (Layer 2 Tunneling Protocol) ja PPTP (Point to Point Tunneling Protocol) ovat siirtoyhteyskerroksen protokollia, jotka molemmat kapseloivat hyötydatan PPP-kehyksiin (Point to Point Protocol) lähetettäväksi välittävän verkon yli. OSI-mallin kerros 3 on verkkokerros, jossa liikenne koostuu paketeista. IPsec on esimerkki verkkokerroksen protokollasta, jota voidaan käyttää tunneloitaessa IP-paketteja välittävän verkon yli.

5.2.1 IPsec

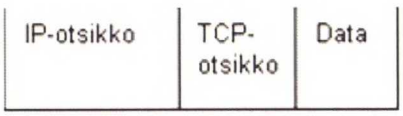
IPsec on suunniteltu IPv4- (Internet Protocol version 4)ja IPv6-protokollia (Internet Protocol Version 6) varten tarjoamaan kryptografiaan perustuvaa korkealaatuista monikäyttöistä tietoturvaa. IPsecin tarjoamat turvapalvelut sisältävät pääsyn hallintaa, yhteydetöntä eheyttä, lähteen todentamista, suojaa toistoja vastaan, luottamuksellisuutta ja rajallista liikennevuon luottamuksellisuutta. Näitä turvapalveluita toteutetaan OSI-mallin verkkokerroksella ja täten ne tarjoavat suojaa verkkokerroksella ja sitä ylemmille tasoille [32]. Järjestelmien suunnittelijoiden ja käyttäjien tehtävänä on valita, mitä turvaominaisuuksia tietyssä järjestelmässä, yhteyksissä ja sovelluksissa halutaan käyttää.

IPsec käyttää tarjoamiensa turvapalveluiden toteuttamiseen kahta protokollaa – Authentication Header (AH) sekä Encapsulating Security Payload (ESP) – ja kryptografisten avainten hallintaprosesseja ja protokollia. Näiden protokollien avulla voidaan tarjota haluttuja tietoturvapalveluita IPv4- ja IPv6-verkoissa. AH- ja ESP-protokollia voidaan käyttää joko erikseen, tai tietyin ehdoin yhdessä. Käytettävä protokolla ja muut yhteydellä käytettävät optiot määritellään yhteydenmuodostuksessa, luotaessa turvasopimusta. Tämä on tarkemmin kuvattu kappaleessa 5.2.1.1.

IPsec koostuu kolmesta perustekijästä, jotka kaikki tukevat IPsecin käyttöä VPN-ratkaisuissa: todennus, salaus ja avaimienhallinta. [32] Todennus on toimenpide, jossa varmistetaan, että datan lähettäjät ovat niitä, joita he antavat ymmärtää olevansa ja että vastaanotettu data on sama, kuin lähetetty data, eli että dataa ei ole muutettu sitä välitettäessä. Salauksessa välitettävä dataa muokataan siten, että ainoastaan tietyn salauksenpurkuavaimen haltijoille data saadaan palautettua ymmärrettävään muotoon. Avaintenhallinta-prosessilla hallitaan lähettäjillä ja vastaanottajilla olevia avaimia.

IPsecin tarjoamia palveluita voidaan käyttää yhteyden päätepisteiden välillä, yhteyden toisen päätepisteen ja tietoturvayhdyskäytävän tai kahden tietoturvayhdyskäytävän välillä [33]. Tietoturvayhdyskäytävällä tarkoitetaan yhteyttä välittävää laitetta, joka toteuttaa IPsec-protokolia. Tietoturvayhdyskäytävinä voivat toimia esimerkiksi reitittimet tai palomuurit, joiden kautta yhteyden päätepisteiden välinen liikenne kulkee.

Seuraavissa kappaleissa esitellään AH- ja ESP-tekniikat, joita käytetään IPsec-protokollassa. ESP ja AH tarjoavat päällekkäisiä palveluita, mutta niiden erona on palveluiden kattavuus IP-paketin kannalta. Näistä AH tarjoaa suojaa myös paketin otsikoille ja ESP ainoastaan siinä tapauksessa, että otsikot ovat ESP-kehyksen sisällä. Sekä autentikointiotsikon että ESP:n tapauksissa lähtökohtana oleva IP-paketti on yksinkertainen IP-paketti, joka koostuu IP-otsikosta, yhteyskerroksen otsikosta ja väliteettävästä hyötytiedosta. Yksinkertaisen IP-paketin rakenne on esitelty kuvassa 6, jossa yhteyskerroksen protokolla on TCP (Transmission Control Protocol).



Kuva 6 Yksinkertainen IP-paketti [34]

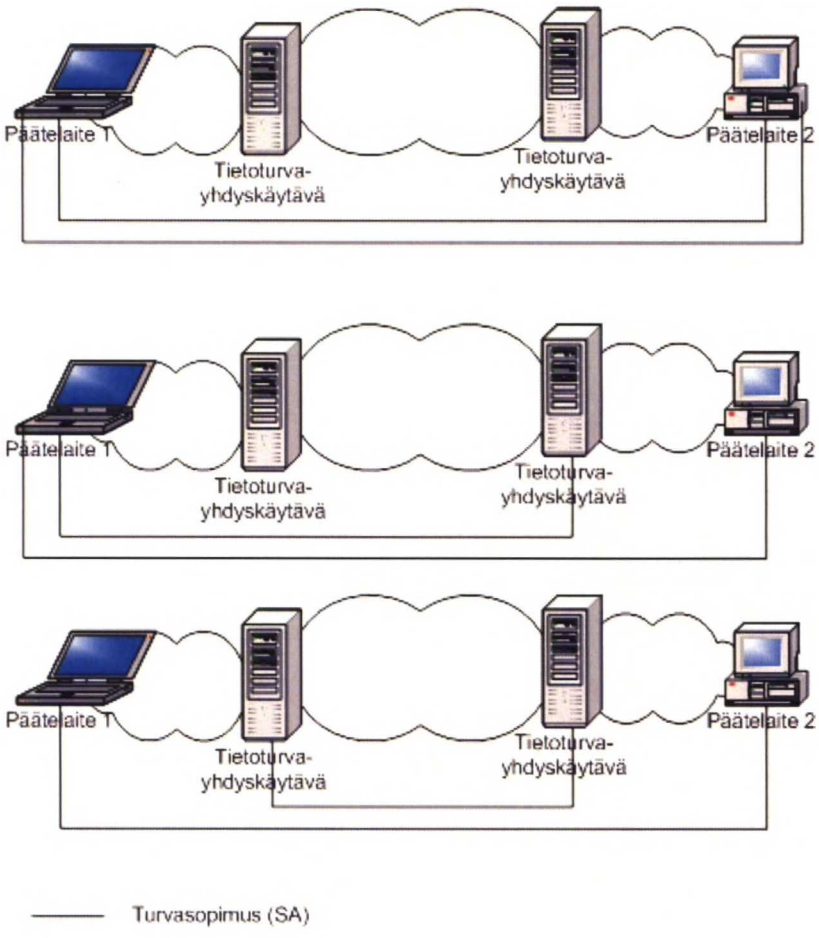
5.2.1.1 Turvasopimus – Security Association (SA)

Turvasopimus on kahden tai useamman laitteen välinen sopimus, joka kuvaa miten tietoturvapalveluita käytetään ja miten laitteiden välisen kommunikaation turvallisuus

toteutetaan. [35] SA on yksisuuntainen yhteys, joka sisältää ehdot ja säännöt, joiden mukaan kahden tai useamman laitteen välinen kommunikointi turvataan. Koska SA on yksisuuntainen, tarvitaan kahden laitteen välistä kommunikointia varten kaksi turvayhteyttä; yksi kumpaankin suuntaan. Yksi turvayhteys voi ottaa käyttöön joko AH:n tai ESP:n, mutta ei molempia. Jos kahden laitteen välisessä kommunikaatiossa halutaan käyttää sekä AH:tä että ESP:tä on muodostettava kaksi turvayhteyttä molempiin liikennöintisuuntiin. [32]

Turvayhteys koostuu kolmikosta, joka tekee turvayhteydestä uniikin sitä käyttävän laitteen kannalta. Turvayhteyden kolmikko sisältää turvaparametri-indeksin (SPI, Security Parameter Index), IP-kohdeosoitteen ja tiedon käytettävästä tietoturvaprotokollasta, joka on joko AH tai ESP. [32] Turvasopimuksella sovitaan laitteiden välisessä kommunikaatiossa käytettävä tietoturvaprotokolla, tämän protokollan optiot ja käytetäänkö tunneli- vai kuljetustilaa. Tunneli- ja kuljetustilan käyttö eri tietoturvaprotokollilla on esitetty kappaleissa 5.2.1.2 ja 5.2.1.3

Useampaa tietoturvayhteyttä on mahdollista käyttää päällekkäin, jolloin voidaan hyödyntää samalla yhteydellä useita eri tietoturvaprotokollia. Kuvassa 7 on esitetty kolme eri tapaa käyttää useampaa turvasopimusta. Ensimmäisellä tavalla toteutetuissa yhteyksissä on mahdollista käyttää ainoastaan kahta päällekkäistä turvasopimusta, koska kahden turvasopimuksen päätepisteet ovat samat. Tällöin ei ole mielekästä käyttää useampia turvasopimuksia, koska ne eivät enää paranna yhteyden turvallisuutta. Jos eri turvayhteyksillä on eri päätepiste tai päätepisteet, on mahdollista käyttää kahta tai useampaa turvasopimusta samalla linkillä. Kuvassa 7 esitetyistä tilanteista kaksi alempaa ovat yksinkertaistuksia tilanteista, jossa voisi käyttää useampaa kuin kahta turvayhteyttä samalla linkillä. Jos kahden laitteen välisellä yhteydellä on useampia turvayhdyskäytäviä, voidaan niiden ja lähteen väleille muodostaa useita turvayhteyksiä.



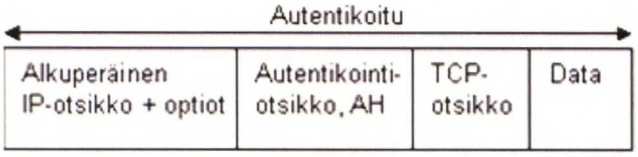
Kuva 7 Päällekkäisten tietoturvasopimusten käyttö [32]

5.2.1.2 IP autentikointiotsikko – Authentication Header (AH)

Autentikointiotsikon avulla tarjotaan yhteydetöntä eheyttä ja datan alkuperän autentikointia IP-paketeille ja turvaa pakettien toisto-hyökkäyksiä vastaan. AH:ta voidaan käyttää yksinään tai ESP:n kanssa yhdessä [34]. ESP esitellään kappaleessa 5.2.1.3.

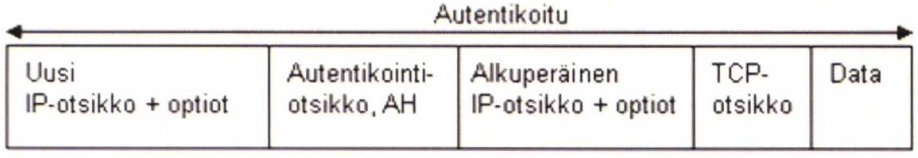
AH:ta voidaan käyttää kahdessa eri tilassa: kuljetus- tai tunnelitilassa. Kuljetustilassa AH sijoitetaan alkuperäisen IP-paketin sisään IP-otsikoiden ja kuljetuskerroksen otsikon väliin. [34] Kuvissa 9 ja 10 kuljetuskerroksen protokolla on TCP. Kuljetustilaa voidaan käyttää ainoastaan yhteyden päätepisteiden välillä ja se tarjoaa tietoturvaa ylemmän

tason protokollille ja tietyille IP-otsikon kentille. Kuvassa 9 on esitetty autentikointiotsikon käyttöä kuljetustilassa IP-paketissa.



Kuva 8 Autentikointiotsikon käyttö kuljetustilassa [34]

Käytettäessä AH:ta tunnelitilassa, alkuperäinen IP-paketti sijoitetaan uuden paketin sisään ja autentikointiotsikko tulee uuden IP-otsikon ja vanhan IP-paketin väliin. Ulompi IP-paketti sisältää tunnelin alku- ja päätepisteiden osoitteet ja sisempi IP-paketti sisältää paketin alkuperäisen lähteen ja kohteen osoitteet. [34] Uloimman ja sisemmän pakettien osoitteet voivat erota toisistaan, jos IPsec-tunneli muodostetaan turvayhdyskäytävässä ja se päättyy toiseen turvayhdyskäytävään. Tällöin ulommassa IP-otsikossa on turvayhdyskäytävien osoitteet, ja sisemmässä paketissa on yhteyden päätepisteiden osoitteet. Tunnelitilassa AH suojaa koko alkuperäisen IP-paketin, mukaan lukien kaikki IP-otsikot [34]. Kuvassa 10 on esitetty autentikointiotsikon käyttöä tunnelitilassa IP-paketissa.



Kuva 9 Autentikointiotsikon käyttö tunnelitilassa [34]

Käytettäessä IPsec AH:ta välitettävä paketti ainoastaan autentikoidaan, eikä välitettävän tiedon luottamuksellisuutta turvata salauksella. AH:n tarkoituksena on taata koko paketin autentikoitavuus ja tämän takia autentikointisumman laskennassa käytetään koko pakettia. [34] Luottamuksellisuuden puute ja koko paketin autentikointi tekevät AH:sta melko hyödyttömän ratkaisun käytettäessä IPsec-tekniikkaa VPN-ratkaisuissa ja erityisesti mobiiliverkoissa. VPN-yhteyksiä käytettäessä on välitettävälle liikenteelle

taattava sekä tiedon autentikoitavuus että luottamuksellisuus. Pelkän autentikointiotsikon käyttö ei riitä täyttämään VPN-yhteyksille asetettavia tietoturvavaatimuksia, mutta IPsec-protokollan muilla mekanismeilla voidaan tarjota sekä autentikoitavuutta että luottamuksellisuutta.

Välitettäessä liikennettä verkko-osoitteen muunnoksen (NAT, Network Address Translation) tekevän laitteen läpi, muutetaan IP-paketin uloimman otsikon lähdeosoitetta, jolloin IP-paketti ei vastaa enää autentikointiotsikossa olevaa tarkistussummaa. Käytännössä AH ei tuo lisäarvoa verrattuna pelkän ESP:n käyttöön, joten IPsec-pohjaisissa VPN-toteutuksissa käytetään lähes poikkeuksetta pelkkää IPsec ESP-tekniikkaa.

5.2.1.3 Encapsulating Security Payload (ESP)

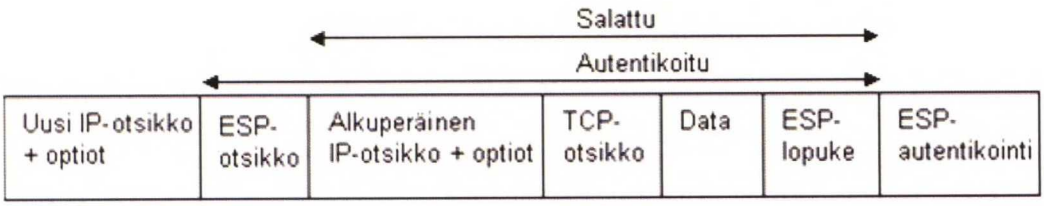
ESP on mekanismi, jolla voidaan tarjota datan luottamuksellisuutta, lähteen autentikointia, yhteydetöntä koskemattomuutta, toistohyökkäyksen estoa ja rajallista liikennevirran koskemattomuutta. Käytettävissä olevat turvapalvelut riippuvat SA:n muodostushetkellä käytetyistä optioista ja järjestelmän implementaatiosta. Käytettäessä ESP:tä voidaan valita käyttöön kaikki tai tietyin ehdoin vain osa turvapalveluista, mutta kaikissa tapauksissa ainakin yksi turvapalveluista on oltava käytössä. [36]

ESP:tä voidaan käyttää kahdessa eri tilassa; kuljetustilassa tai tunnelitilassa. Kuljetustilassa alkuperäisen paketin IP-otsikoiden ja kuljetuskerroksen otsikoiden (esimerkiksi TCP tai UDP (User Datagram Protocol)) väliin sijoitetaan ESP-otsikko ja paketin loppuun ESP-lopuke (ESP-footer) ja ESP- autentikointitietue. [36] Kuljetustilassa alkuperäisen IP-paketin hyötykuorma, eli ylempien kerrosten otsikot ja välitettävä data salataan ja salatun datan lisäksi ESP-otsikko autentikoidaan. ESP-tilassa käytetään paketin IP-otsikkona paketin alkuperäistä otsikkoa, jolloin paketin lähde- ja kohdetiedot eivät ole salattuja – ainoastaan välitettävä data salataan. Kuljetustila on käytettävissä ainoastaan isäntäkoneille toteutettavissa sovelluksissa. Kuljetustilassa säästetään tunnelitilaan verrattuna käytettävää siirtokaistaa, koska välitettävänä ei ole

salattuja IP-otsikoita. Kuvassa 11 on esitetty IP-paketin rakenne käytettäessä ESP:tä kuljetustilassa ja autentikointia.

Kuva 10 ESP:n käyttö kuljetustilassa [36]

Tunnelitilassa ESP suojaa sisemmän IP-paketin kokonaan mukaan lukien paketin hyötykuorman ja IP-otsikot. Sisempi IP-otsikko sisältää alkuperäisen lähteen ja lopullisen paketin kohteen ja uloimmassa IP-otsikossa voi olla edellisistä otsikoista poikkeavat osoitteet, kuten tietoturvayhdyskäytävien osoitteet. [36] Uloimmaista IP-otsikkoa käytetään reititettäessä paketti IPsec-tunnelin luontipisteestä joko vastanottajalle saakka tai tietylle tietoturvayhdyskäytävälle, josta sisempi paketti reititetään alkuperäiseen kohteeseen. Tunnelitilassa alkuperäinen paketti on salattu kokonaisuudessaan ja kuten kuljetustilassakin salatun osan lisäksi ESP-otsikko on autentikoitu. Tunnelitilaa voidaan hyödyntää sekä isäntäkoneissa että tietoturvayhdyskäytävissä. Kuvassa 12 on esitetty IP-paketin rakenne käytettäessä autentikointia ja ESP:tä tunnelitilassa.



Kuva 11 ESP:n käyttö tunnelitilassa [36]

IP-reitityksessä paketteja saatetaan fragmentoida, jos jokin verkko ei voi välittää tietyn suuruisia paketteja. Jokaiselle verkolle on määritelty suurin mahdollinen siirtoyksikkö (MTU, Maximum Transfer Unit), joka vastaa verkon suorituskykyä. Paketeille voidaan

tehdä fragmentointi ESP-prosessoinin jälkeen IPsec-prosessin sisällä [36]. Koska ESP:n kuljetustilan prosessointi suoritetaan yhteyden päätepisteissä, voidaan sitä käyttää ainoastaan fragmentoimattomiin IP-paketteihin. Kuljetustilassa välitettyjä paketteja voidaan myöhemmin fragmentoida, jonka jälkeen ne pitää koota kohteessa ennen ESP-prosessointia. ESP:n tunnelitilaa voidaan käyttää tietoturvayhdyskäytävissä kaikkiin IP-paketteihin fragmentoinnista huolimatta.

5.2.1.4 Avaimien hallinta – Internet Key Exchange (IKE)

Manuaalinen avaimien hallinta, jossa jokaiseen järjestelmään asetetaan sen omat ja muiden järjestelmien avaimet, on yksinkertaisin tapa hallita avaimia. Manuaalinen avaimien hallinta voi olla käytännöllinen pienissä staattisissa verkoissa, mutta sitä ei voida käyttää keskisuurissa tai suurissa järjestelmissä huonon skaalautuvuutensa vuoksi. Manuaalisen avaimien hallinnan käyttö voi olla perusteltua myös tilanteissa, joissa ainoastaan rajallinen määrä yhteyksiä pitää suojata. Käytettäessä IPsec-protokollaa, voidaan IKE-protokollan (Internet Key Exchange) avulla salausavaimia hallita automaattisesti.

IKE-protokolla on hybridi-protokolla, joka toteuttaa Oakley ja Skeme avaintenvaihtojärjestelmät ja ISAKMP:n (Internet Security Association and Key Management Protocol) määrittelemän kehyksen. Tästä syystä IKE:stä käytetään myös nimeä ISAKMP/Oakley. IKE-protokollaa käytetään IPsec-protokollan yhteydessä avaintenhallintaan ja turvasopimusten muodostamiseen. IPsec-protokollaan voidaan käyttää ilman IKE-protokollaa, mutta IKE:n käyttö tuo IPsec-protokollaan lisää ominaisuuksia, joustavuutta ja helpottaa protokollan käyttöä. IKE:n tehtävänä on neuvotella ja tarjota autentikoituja salausavaimia IPsec-protokollan turvasopimusta varten. IKE neuvottelee automaattisesti muodostettavan IPsec turvayhteyden ja mahdollistaa IPsec-protokollan suojaaman liikennöinnin ilman manuaalista konfigurointia. [36] IKE:n tuomat edut IPsec-protokollan käyttöön ovat:

- IPsec-protokollan parametreja ei tarvitse manuaalisesti asettaa kommunikoiviin laitteisiin
- IPsec-turvayhteyden elinikä pystytään asettamaan
- Salausavaimia on mahdollista vaihtaa yhteyden aikana
- Mahdollistaa toistoneston käyttämisen IPsec-protokollassa
- Mahdollistaa laitteiden dynaamisen autentikoinnin. [37]

IKE-protokollan toiminta muodostuu kahdesta eri vaiheesta, joista ensimmäisessä määritellään turvallinen kanava neuvottelevien laitteiden välille ja toisessa vaiheessa muodostetaan IPsec-protokollan tarvitsemat salausavaimet ja neuvotellaan turvayhteys. Ensimmäisestä vaiheesta voidaan käyttää nimeä IKE SA:n muodostamiseksi ja sillä turvataan tulevat toisen vaiheen IKE-neuvottelut. Toisessa vaiheessa määritellään IPsec-protokollan turvayhteyden parametrit eli muodostetaan turvayhteys. Toisessa vaiheessa on turvayhteyden muodostamisen lisäksi mahdollista neuvotella uudet salausavaimet. [35][38]

5.2.2 L2TP – Layer 2 Tunneling Protocol

L2TP on IETF:n standardoima tunnelointiprotokolla, joka seuraa kehityksessä kahta aikaisempaa tunnelointiprotokollaa; PPTP ja L2F (Layer 2 Forwarding). PPTP oli alun perin Microsoftin kehittämä protokolla ja on edelleen käytössä Microsoftin VPN-ratkaisuissa. L2TP:n tehtävänä on tunneloida PPP-yhteyksiä minkä tahansa siirtoverkon yli. L2TP ja PPP ovat molemmat siirtoyhteyskerroksen protokollia ja niitä käytetään yhdessä muodostamaan yhteys käyttäjän ja kohdepalvelimen välille. L2TP:n tuoma etu PPP-protokollan yhteydessä aikaisemmin käytettyyn siirtoyhteyskerroksen tunnelointiin on mahdollisuus päättää L2TP-tunneli ja PPP-yhteys eri pisteisiin. Kahden solmun välinen yhteys muodostetaan kolmessa vaiheessa. Nämä kolme vaihetta ovat:

- Yhteyttä muodostava päätelaite avaa PPP-yhteyden verkkoyhteyttä tarjoavan operaattorin NAS-palvelimeen
- Muodostetaan yhteys L2TP-tunnelin kohteena olevaan palvelimeen, jolloin välittävän verkon yli kulkeva yhteys näyttää yhdeltä linkiltä siirtoyhteyskerroksen tasolla
- Muodostetaan uusi PPP-yhteys, joka ulottuu kohteeseen saakka L2TP-tunnelin päällä. [31]

Tunnelin muodostuksessa on kaksi vaihtoehtoa; vapaaehtoinen ja pakollinen tila. Vapaaehtoisessa tilassa L2TP-tunneli muodostetaan päätelaitteesta kotiverkon L2TP-tunnelin päätepisteenä toimivaan NAS-palvelimeen. Vapaaehtoisessa tilassa käyttäjä voi valita muodostetaanko tunneli vai ei. Pakollisessa tilassa L2TP-tunneli muodostetaan käyttäjän liityntäverkon NAS-palvelimelta kohdeverkon NAS-palvelimelle käyttäjästä riippumatta. Vapaaehtoisessa tilassa käytettäessä L2TP näkyy käyttäjälle valintamahdollisuuden kautta, mutta pakollisessa tilassa L2TP-tunnelointi on käyttäjän kannalta täysin näkymätön. [31]

VPN-ratkaisuiden yhteydessä L2TP:tä voidaan käyttää suojatun yhteyden muodostamiseen käyttäjän liityntäverkosta käyttäjän kotiverkon NAS-palvelimelle. L2TP:n yhteydessä voidaan käyttää IPsec-protokollaa suojaamaan välitettävää liikennettä tietoturvauhilta. L2TP-tunnelointia voidaan käyttää myös pakettikytkentäisissä matkapuhelinverkoissa toteutettavissa VPN-ratkaisuissa Yrityksen käyttäessä dedikoitua APN-osoitetta, voidaan liikenne GGSN:n ja yrityksen verkon välillä tunneloida käyttäen L2TP-protokollaa. Tällöin GGSN:n ohjaa kaiken tietyn yrityksen liikenteen yrityskohtaiseen L2TP-tunneliin, jonka kautta liikenne välittyy yrityksen omaan verkkoon.

L2TP-protokolla ja PPP-protokollan autentikointi ja salaus eivät täytä IETF:n *Securing L2TP using IPsec*-dokumentissa L2TP-protokollalle määriteltyjä tietoturvallisuutta

koskevia vaatimuksia, joten L2TP:n kanssa on käytettävä erillisiä turvamekanismeja liikenteen suojaamiseksi [39]. L2TP:n tunnelin liikenne on jaettu hallinta- ja dataliikenteeseen, jotka molemmat on suojattava sekä tietovuon että yksittäisten pakettien tasolla. Kun välittävänä verkkona on IP-verkko, on L2TP:n turvavaatimusten täyttämiseksi käytettävä IPsec ESP-protokollaa, jolla pystytään tarjoamaan sekä hallinta että dataliikenteelle vaatimusten mukainen turvataso. Suojattaessa L2TP-tunnelia IPsec-protokollalla, ei tunnelin sisällä olevaa liikennettä ole vielä suojattu, jolloin myös tunnelissa välitettävän liikenteen suojaamiseen voidaan käyttää IPsec-protokolla.

5.2.3 UDP-kapselointi

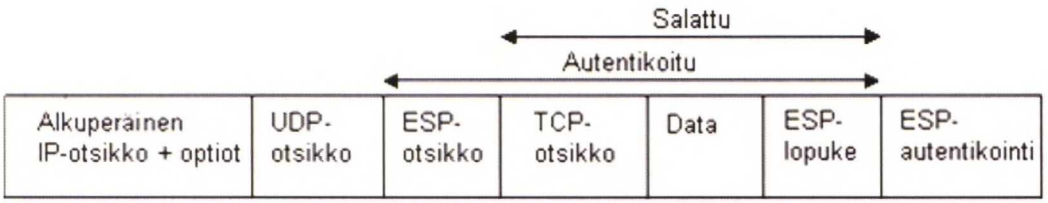
Verkko-osoitteen muutosta käytetään laajasti Internetissä yhteyksien jakamiseen usean käyttäjän kesken. Monissa liityntäyhteyksiä tarjoavien tietoliikenneoperaattoreiden verkoissa, julkisissa langattomissa lähiverkoissa ja yritysten lähiverkoissa käytetään verkko-osoitteen muunnosta, mutta myös mobiilioperaattorit käyttävät verkko-osoitteen muunnosta GPRS-tilaajiensa Internet-yhteyksissä.

Verkko-osoitteiden muunnosta käyttävistä verkoista estyy Internetiin suuntautuva liikenne niiltä käyttäjiltä, jotka käyttävät L2TP- tai IPsec-protokolliin perustuvia VPN-ratkaisuja, tai joiden liikenne on suojattu käyttäen IPsec-protokollan tunnelitilaa [40]. Liikennöinti verkko-osoitteen muunnoksessa IP-pakettien otsikkokenttiä muutetaan, jolloin pakettien autentikoitu osa muuttuu, eikä paketeissa oleva autentikointisumma vastaa alkuperäisen paketin summaa. Autentikointisumman muuttuessa paketin vastaanottaja hylkää sen, koska paketin sisäiset tiedot ovat muuttuneet ja paketin luottamuksellisuus on vaarantunut. IETF on ratkaissut tämän ongelman määrittelemällä menetelmän, jolla IPsec ESP-protokollan liikenne kapseloidaan UDP-pakettien sisään. Toteuttamalla UDP-kapselointi IETF:n määrittelemällä tavalla, voidaan sekä IPsec-liikenne että IPsec-protokollalla suojattu L2TP-liikenne välittää verkko-osoitteen muunnoksen tekevän solmun kautta. Ehtona menetelmä toimimiselle on, että verkko-osoitteen muunnoksen tekevä solmu sallii UDP-liikenteen kauttakulun ja sekä liikenteen

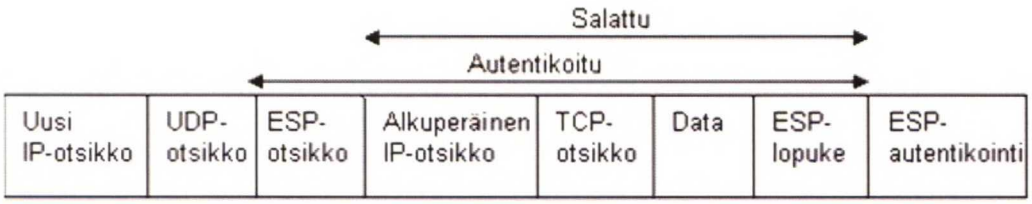
lähettäjä että vastaanottaja tukevat tätä menetelmää. UDP-kapseloinnin käyttö neuvotellaan yhteyden muodostusvaiheessa IKE-protokollan avulla [40].

Kappaleessa 5.2.1.3 käsiteltiin IP ESP:n toimintaa, jota UDP-kapselointi täydentää mahdollistaen pakettien välittämisen verkko-osoitteen muunnoksen suorittavien laitteiden kautta. Kuvassa 1 on kuvattu yksinkertainen IP-paketti, ennen IPsec-protokollien vaikutusta ja kuvissa 4 ja 5 ESP:n käyttöä tunneli- ja kuljetustiloissa. Kuvan 1 paketista on päästy kuvien 4 ja 5 paketteihin käyttämällä ESP:tä ja nyt ESP:n lisäksi hyödynnetään UDP-kapselointia.

UDP-kapseloinnissa IP-paketin uloimman IP-otsikon jälkeen sijoitetaan uusi UDP-otsikko ja uloimmassa IP-otsikossa muutetaan paketin pituus-, protokolla- ja otsikon tarkistussummakenttiä vastaamaan uusia arvoja. Kuvassa 13 on esitetty IP-paketti, jossa on käytetty ESP:tä kuljetustilassa ja joka on UDP-kapseloitu. Kuvassa 14 on vastaavasti käytetty ESP:tä tunnelitilassa ja UDP-kapselointia.



Kuva 12 ESP:n ja UDP-kapseloinnin käyttö kuljetustilassa [36]



Kuva 13 ESP:n ja UDP-kapseloinnin käyttö tunnelitilassa [36]

5.2.4 PPTP – Point to Point Tunneling Protocol

PPTP on usean yrityksen muodostaman konsortion kehittämä protokolla, jota käytetään PPP-protokollan tunneloimiseen IP-verkon yli. Osittain samoihin tarkoituksiin voidaan käyttää IETF:n määrittelemää L2TP-protokollaa. Vaikka PPTP ei ole IETF:n määrittelemä protokolla, on se esitetty IETF:n informatiivisena RFC-dokumenttina. Vaikka PPTP ei ole standardoitu protokolla, on sillä edelleen merkitystä, koska Microsoftin käyttöjärjestelmät tukevat protokollan käyttöä. Microsoft tukee myös muita tunnelointiin käytettäviä protokollia, kuten L2TP:tä.

PPTP-protokolla toimii asiakas-palvelin mallin mukaisesti, jossa päätelaitteen ja kohdeverkossa olevan PPTP-verkkopalvelimen välille muodostetaan yhteys. Muodostetun PPTP-yhteyden päälle muodostettaan uusi PPP-yhteys, jota käytetään kuten normaalin PPP-yhteyden tapaan. PPP-yhteyden tunneloinnissa PPTP käyttää pohjana GRE:n (General Routing Encapsulation) määrittelemään kapselointia kuitenkin täydentäen sitä. PPTP ei sisällä omia autentikointimenetelmiä, vaan sitä käytettäessä turvaudutaan PPP:n tarjoamiin mekanismeihin. [41] PPTP-protokollan merkitys vähenee

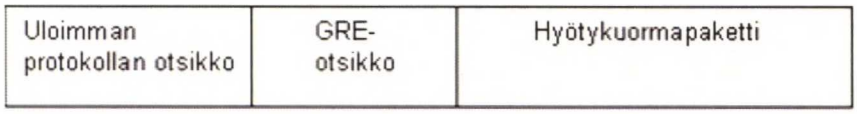
entisestään, koska Microsoft tukee myös uudempaa L2TP-protokollaa, [42] jonka takia PPTP:n toimintaa ei esitellä tarkemmin tässä työssä.

5.2.5 GRE – Generic Routing Encapsulation

GRE:n suunnittelun tarkoituksena oli tarjota yleinen tapa kapseloida verkkokerroksen protokollaa toisen verkkokerroksen protokollan sisään. Sen sijaan, että suunniteltaisiin jokaista kapseloitavaa protokollaparia varten uudet käytännöt, käytettäisiin yleistä kapselointimekanismia. GRE ei siis tarjoa valmista mekanismia tiettyjen protokollien kapselointiin, vaan kuvaa yleiskäyttöisen tavan kapseloida protokollia sisäkkäin. VPN-protokollista sekä IPsec että PPTP käyttävät GRE:n määrittelemää kapselointitapaa. [43][44]

Yleisimmässä tapauksessa järjestelmällä on paketti, joka pitää kapseloida ja toimittaa tiettyyn kohteeseen. Tätä välitettävää paketti kutsutaan hyötykuormapaketiksi. Käytettäessä GRE:tä hyötykuormapaketti kapseloidaan ensin GRE-pakettiin ja sen jälkeen jonkin toisen protokollan mukaiseen pakettiin. Uloimman protokollan tehtävänä on huolehtia koko paketin välityksestä kohteeseen. Kuvassa 15 on esitetty hyötykuormapaketin kapseloimista GRE- ja uloimman protokollan-paketteihin. GRE:tä voidaan hyödyntää peittämällä tietty osa verkosta kahden solmun välillä. Tunneloitaessa liikenne GRE:n mukaisesti kahden pisteen välillä, näyttää tunneli sisimmän protokollan kannalta yhdeltä linkiltä. [43]

Käytännössä GRE:tä voidaan käyttää esimerkiksi tunneloimaan IP-paketteja IP-pakettien sisään, jolloin voidaan yhdistää kaksi fyysisesti erillään olevaa verkkoa siten, että molemmissa on käytössä yksityiset IP-osoitteet ja verkot ovat loogisesti samaa verkkoa. Tämän tyyppisellä IP-tunneloinnilla peitetään yksityisen verkon osoitteita käyttäviltä päätelaitteilta pakettien reititys julkisen Internetin yli. IP-paketteja voidaan kapseloida suoraan toisen IP-paketin sisään, jolloin puhutaan IPinIP-tunneloinnista. GRE:n tarkoituksena on tarjota yleispätevä protokolla vastaavaan tunnelointiin riippumatta sisemmästä tai uloimmasta protokollasta.



Kuva 14 GRE-protokollan käyttö kapseloinnissa [43]

GRE ei itsessään takaa välitettävälle liikenteelle tietoturvaa, vaan tähän tarkoitukseen on käytettävä sitä tarkoitusta varten suunniteltuja protokollia, kuten IPsec-protokollaa.

5.2.6 SSL-tekniikkaan perustuvat VPN-ratkaisut

SSL-tekniikka (Secure Socket Layer) on Netscape Communications Corporate:n kehittämä tekniikka, jolla voidaan suojata Internetissä muodostettavia yhteyksiä. SSL protokolla tarjoaa seuraavia tietoturvapalveluita:

- Välitettävän tiedon salaaminen
- Palvelimen autentikointi
- Välitettävien viestien eheys
- Asiakkaiden autentikointi TCP/IP-yhteyksillä, joka on vaihtoehtoinen palvelu. [45]

SSL-tekniikkaa käytetään OSI-mallin mukaisesti sovellus ja yhteystapatasoilla. SSL-yhteys muodostetaan SSL-asiakasohjelman ja yksityisverkossa olevan SSL-palvelimen välille. Tällöin muodostetaan yhteystapakerroksella kahden pisteen välinen TCP/IP-yhteys, jonka päällä SSL-tekniikkaa hyödyntävät sovellukset toimivat. [4] Ainoastaan yksi sovellus voi käyttää yhtä SSL-yhteyttä, joten jokaista eri sovellusta varten on muodostettava oma SSL-yhteys.

SSL-tekniikka on käytössä useimmissa Internet-selainohjelmissa ja sitä käytetään turvallisia yhteyksiä vaativissa Internet-sovelluksissa, kuten Internet-pankeissa ja yhteyksissä yritysten sisäisiin palveluihin, kuten sähköpostiin ja yrityksen tietokantoihin.

SSL-tekniikalla voidaan tarjota IP-protokollaan perustuvien VPN-ratkaisuiden kaltaisia palveluita, mutta SSL ei silti ole VPN-tekniikka termin varsinaisessa merkityksessä, koska SSL ei liitä tietokonetta osaksi yksityisverkkoa, vaan ainoastaan tarjoaa turvallisen yhteyden rajattuihin yksityisverkon palveluihin. [4] SSL-tekniikan pohjalta on kehitetty IETF:n standardoima uusi TLS-protokolla (Transport Layer Security), joka pohjautuu SSL-protokollan versioon 3.0. TLS- ja SSL-protokollien erot eivät ole merkittävät, mutta ne eivät kuitenkaan ole yhteensopivia [46]. TLS-protokolla toimii SSL-protokollan tavoin ja sitä käyttäen voidaan toteuttaa vastaavantyyppisiä VPN-ratkaisuiden kaltaisia palveluita, kuten SSL-protokollallakin.

5.2.7 Tunnelointiprotokollien aiheuttama lisäkuorma

Tunnelointiprotokollissa alkuperäisen IP-liikenteen otsikkotietoja muokataan tai otsikoihin lisätään ylimääräisiä kenttiä. Lisäykset johtuvat käytetyistä salausalgoritmeista ja käytettävien tunnelointiprotokollien otsikoista. Näillä lisäyksillä ja muutoksilla voi olla merkittäviä vaikutuksia käyttäjien kokeman palvelunlaatuun, jos käytettävä protokollan tuottama lisäkuorma on suuri ja jos tietoliikenneyhteyden kaistanleveys on kokonaan käytössä. Tällaisessa tapauksessa otsikkokenttien lisäys on pois välitettävästä hyötykuormasta, jolloin käyttäjän havaitsema tiedonsiirtonopeus alenee. Käytettävien IP-pakettien koko vaikuttaa lisäysten vaikutuksen merkittävyyteen. Käytettäessä pieniä paketteja, on lisäys suhteellisesti suurempi, kuin isoilla paketeilla. Käytettäessä 1500 tavun IP-paketteja on IPsec-protokollan aiheuttama lisäkuorma 1,5 – 7 % koko liikenteen määrästä. [47] Jos yhteyden koko kapasiteettia ei käytetä, vaikuttaa tunnelointiprotokollan käyttö ainoastaan välitettävän liikenteen määrään, mutta ei käyttäjän kokemaan laatuun.

Pakettikytkentäisissä matkapuhelinverkoissa pullonkaula kaistanleveyden suhteen on radioverkko, jonka tiedonsiirtonopeuden mukaan koko yhteyden nopeus määräytyy. Langattomissa lähiverkoissa pullonkaulana toimii usein liityntäverkko, jonka kaistanleveys on radioverkon kaistanleveyttä huomattavasti alhaisempi. Liityntäverkon

kaistanleveys on usein langattoman lähiverkon kaistanleveyttä alhaisempi kodeissa olevissa verkoissa, joissa liityntäyhteytenä on usein DSL-yhteys tai muu vastaava yhteys. Myös Hot Spot verkoissa käytetään myös liityntäyhteyksiä, joiden kaistanleveys on radioverkon kaistanleveyttä alhaisempi. Tämän ongelman merkitys kasvaa entisestään, kun samaa verkkoa käyttää useampi käyttäjä. Usean käyttäjän tilanteessa radioverkon kapasiteetti on riittävä, mutta molempien käyttäjien liikenne välitetään verkon ulkopuolelle samalla liityntäyhteydellä. Yrityksen lähiverkkoihin liitettävissä langattomissa verkoissa tämä ongelma ei ole merkittävä, koska osa käytettävistä verkkopalveluista sijaitsee lähiverkossa ja liityntäyhteyden kapasiteetin on oltava riittävä riippumatta tavasta, jolla yksittäiset päätelaitteet liitetään lähiverkkoon.

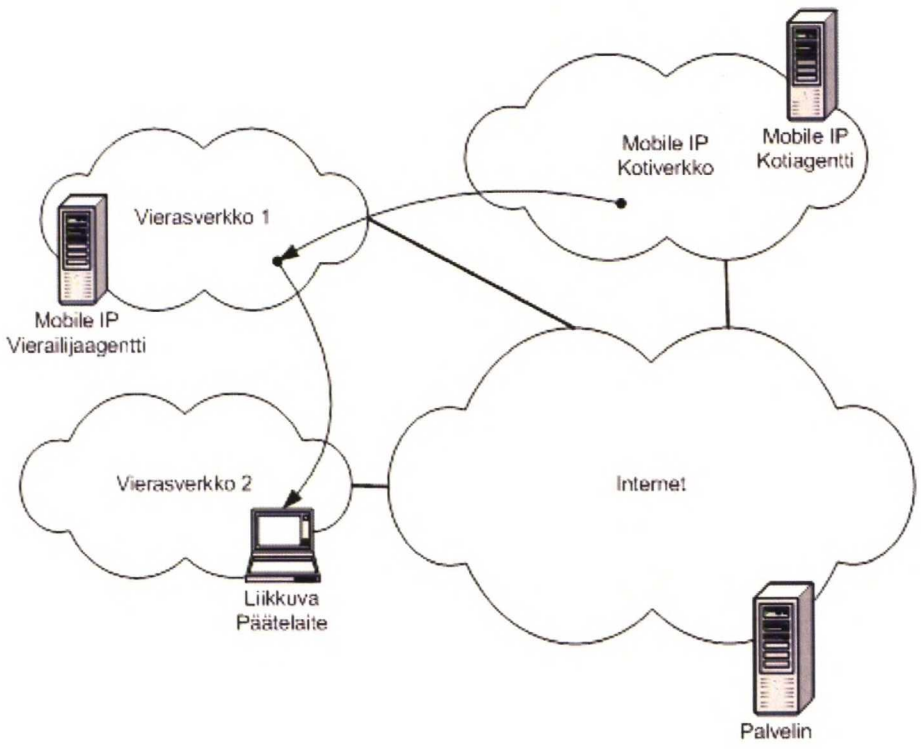
Tietoliikenteen hyötysuhteen lisäksi tunnelointiprotokollien aiheuttama lisäkuorma voi vaikuttaa yhteyden käytöstä aiheutuviin kustannuksiin. Pakettikytkentäisissä matkapuhelinverkoissa dataliikenteen laskutus on usein toteutettu liikennemäärään pohjautuvasti. Kuten kappaleessa 2.1.2 ja 2.1.3 on esitetty, pakettikytkentäisissä matkapuhelinverkoissa laskutus tapahtuu SGSN ja GGSN-palvelimissa operaattorin runkoverkossa. Jos tunnelointiprotokollaa käytetään päätelaitteen ja yritysverkon välillä, eli liikenne välitetään tunneloituna operaattorin runkoverkossa, lisää se liikennemäärään pohjautuvia kustannuksia. Jos käyttäjien liikenne tunneloidaan vasta laskutusta suorittavien palvelimien jälkeen, ei tunnelointiprotokollan käyttö vaikuta suoraan kustannuksiin.

5.3 Mobile IP ja VPN

Mobile IP on IETF:n määrittelemä protokolla, jolla voidaan toteuttaa saumaton liikkuvuus IP-aliverkkojen ja tiedonsiirtokanavien välillä. Mobile IP-protokolla määrittelee IP-protokollaan laajennuksen, jonka avulla IP-paketteja voidaan reitittää liikkuvalle päätelaitteelle. [48] Tässä yhteydessä liikkuvuudella tarkoitetaan päätelaitteen liikkumista IP-aliverkkojen välillä. Päätelaitteen liikkuvuus yhden langattoman verkon sisällä on toteutettu verkkokohtaisilla ratkaisuilla OSI-mallin

siirtoyhteys ja fyysisellä kerroksella. Mobile IP-protokolla toimii verkkokerroksella ja on siis erillinen langattomien verkkojen liikkuvuudenhallinnasta.

Mobile IP-arkkitehtuuri muodostuu Mobile IP kotiagenteista (Home Agent, HA), huoltoagenteista (Foreign Agent, FA) ja asiakasohjelmistoista. Arkkitehtuurissa käyttäjälle on määritelty yksi kotiverkko, jossa käyttäjän kotiagentti sijaitsee. Kuvan 15 mukaisessa arkkitehtuurissa yksi liikkuva päätelaite siirtyy kolmen eri verkon välillä. Ensimmäinen verkko on käyttäjän kotiverkko, jossa toimii Mobile IP-kotiagentti. Käyttäjän siirtyessä vierasverkkoon, jossa on käytössä Mobile IP-vierasagentti, ottaa päätelaite käyttöön vierasagentin huolto-osoitteen (COA, Care Of Address) ja ilmoittaa sen kotiagentille. Toisessa siirtymässä käyttäjä siirtyy vierasverkosta toiseen. Uudessa vierasverkossa ei ole käytössä Mobile IP-vierasagenttia, jolloin päätelaite ottaa käyttöön paikallistavan huolto-osoitteen, joka on käytännössä päätelaitteen verkosta saama IP-osoite.



Kuva 15 Mobile IP arkkitehtuuri

Mobile IP-palvelun tarjoavissa verkoissa on vierasagentti, jonka tehtävänä on huolto-osoitteiden jako omalla alueellaan vieraileville liikkuville päätelaitteille. Huolto-osoite kertoo päätelaitteen sen hetkisen sijainnin ja se vaihtuu joka kerta, kun päätelaite liikkuu uuden vierasverkon alueelle. Päätelaitteen kotiverkossa on kotiagentti, jolle päätelaite ilmoittaa vierasverkon rekisteröitymisen yhteydessä saamansa huolto-osoitteen. Näin kotiagentti aina tietää päätelaitteen senhetkisen sijainnin. Tavallisesti sekä koti- että vierasagenttina toimii normaali reititin, mutta myös erillisiä Mobile IP-palvelimia käytetään. [4]

Kuvan 16 mukaisessa arkkitehtuurissa voidaan kuvitella tilanne, jossa liikkuva päätelaite on yhteydessä Internetiin kytkettyyn palvelimeen. Liikkuvan päätelaitteen siirtyessä verkkojen välillä kotiagentti ylläpitää tietoa liikkuvan päätelaitteen sijainnista. Liikkuvan päätelaite tunneloi paketit kotiagentille, joka lähettää paketit alkuperäiselle kohteelle julkisen Internetin kautta. Jos kuvassa oleva palvelin haluaa muodostaa

yhteyden liikkuvaan päätelaitteeseen, se lähettää paketit liikkuvan päätelaitteen kotiosoitteeseen, jolloin kotiagentti vastaanottaa paketit ja tunneloi ne liikkuvan päätelaitteen ilmoittamaan huolto-osoitteeseen. [4]

Mobile IP ratkaisee liikkuvuuden ongelman ottamalla vakituisen IP-osoitteen rinnalle käyttöön huolto-osoitteen. Huolto-osoite kertoo päätelaitteen senhetkisen sijainnin ja se vaihtuu joka kerta, kun päätelaite siirtyy IP-aliverkosta toiseen. Huolto-osoitteen vaihtuessa päätelaite ilmoittaa kotiagentille uuden huolto-osoitteen, joka on joko käytettävässä IP-aliverkossa olevan Mobile IP vierasagentin IP-osoite tai jos vierasagenttia ei ole, niin päätelaitteen saama IP-osoite. [4] Mobile IP-protokolla toimii siten, että kotiagentti pitää yllä tietoa päätelaitteiden huolto-osoitteista ja ohjaa päätelaitteilla saapuvat paketit päätelaitteiden huolto-osoitteeseen. Mobile IP-tekniikkaa käyttävät päätelaitteet ovat siten saavutettavissa muuttumattomasta IP-osoitteesta, vaikka päätelaite liikkuukin IP-aliverkkojen välillä.

Mobile IP-tekniikkaa voidaan hyödyntää VPN-ratkaisuiden kanssa tarjoamalla käyttäjille katkeamattomat ja kulloinkin parhaat mahdolliset yhteydet yrityksen tietoverkkoon. Päätelaitteessa voi olla mahdollista käyttää useita eri yhteystekniikoita, kuten mobiiliverkkojen yhteyksiä, langattomia lähiverkkoja, kiinteitä lähiverkkoja ja kiinteitä laajakaistayhteyksiä. Mobile IP-tekniikan avulla käyttäjän ei tarvitse muodostaa kuin yksi VPN-yhteys yrityksen tietoverkkoon ja Mobile IP:n ansiosta yhteys säilyy, vaikka käytettävä liityntätekniikka vaihtuisikin. Mobile IP voi valita käytettävissä olevista yhteyksistä kulloinkin parhaan mahdollisen yhteystekniikan, eikä käyttäjän tarvitse muodostaa yhteyttä uudelleen yhteystekniikan vaihtuessa.

5.4 Päätelaitteet käytettäessä virtuaalisia yksityisverkkoja

Päätelaitteet ovat tärkeässä roolissa käsiteltäessä mobiiliyhteyksiä yrityksen tietoverkkoon, koska päätelaitteet määrittelevät mitä ratkaisuja ja mitä tekniikoita on mahdollista käyttää. Päätelaitteiden ominaisuuksista riippuu sekä palveluiden

käytettävyys että sen tekniset mahdollisuudet tietoturvan ja verkkoteknologioiden osilta. Erityyppiset päätelaitteet mahdollistavat erityyppisten sovellusten ja verkkoyhteyksien käytön. Tässä kappaleessa jaetaan päätelaitteet kolmeen eri luokkaan: kannettavat tietokoneet, kämmentietokoneet ja älypuhelimet ja esitellään niiden käyttömahdollisuuksia yritysverkkojen mobiiliyhteyksien kannalta.

5.4.1 Kannettava tietokone

Kannettavat tietokoneet ovat teknisiltä ominaisuuksiltaan ja lisälaitteiden liitäntämahdollisuuksiltaan vertailulaitteista tehokkaimpia ja monipuolisimpia. Kannettavaan tietokoneeseen on mahdollista liittää erilaisia lisälaitteita, joiden avulla voidaan muodostaa mobiiliyhteyksiä useiden langattomien verkkojen kautta. Kannettaviin tietokoneisiin voidaan liittää langattomien lähiverkkojen käytön mahdollistava WLAN-kortti ja uusimmissa kannettavissa tietokoneissa on integroitu WLAN-radio, jonka avulla langattomia lähiverkkoja voidaan käyttää ilman lisälaitteita. Matkapuhelinverkkojen data-yhteyksiä voi hyödyntää kannettavalla tietokoneella liittämällä puhelin tai PCMCIA-kortti (Personal Computer Memory Card International Association) kannettavaan tietokoneeseen. GPRS-puhelimia voi liittää kannettavaan tietokoneeseen infrapuna- tai bluetooth-tekniikalla, tai sopivalla kaapelilla. EDGE- tai UMTS-kykyisiä puhelimia tai kortteja ei ole vielä Suomessa markkinoilla, mutta käyttöönoton ja käytön kannalta ne ovat vastaavien GPRS-päätelaitteiden kaltaisia.

5.4.2 Kämmentietokoneet

Kämmentietokoneet eli PDA-laitteet (Personal Digital Assistant) ovat kannettavia tietokoneita huomattavasti pienempiä laitteita, joiden prosessoriteho, muistikapasiteetti ja lisälaitteiden liitäntämahdollisuudet voivat rajoittaa niiden käytettävyyttä. Kämmentietokoneissa on usein älypuhelimia suurempi näyttö ja niitä on tarkoitus käyttää kahdella kädellä. Useisiin kämmentietokoneisiin on mahdollista liittää lisälaitteita, kuten GPRS-puhelin tai langattomien lähiverkkojen käytön mahdollistava

WLAN-kortti. Nämä lisälaitteet mahdollistavat mobiiliyhteyden muodostamisen yritysverkon ja kämmentietokoneen välille.

Kämmentietokoneiden käyttöjärjestelmät ovat usein normaaleissa tietokoneissa käytettävien käyttöjärjestelmien karsittuja versiota, joten niiden ominaisuudetkin ovat rajallisemmat. Kämmentietokoneissa käytetään yleisesti seuraavia käyttöjärjestelmiä: Windows Mobile 2003, Palm OS, Symbian OS ja Linux-käyttöjärjestelmään perustuvat kämmentietokoneille tarkoitetut käyttöjärjestelmät. Käyttöjärjestelmän tavoin myös asennettavien ohjelmistojen tulee olla kyseistä kämmentietokonetta varten suunniteltuja. [48]

5.4.3 Älypuhelimet

Älypuhelimilla tarkoitetaan kehittyneitä matkapuhelimia, jotka mahdollistavat normaalia matkapuhelinta monipuolisempien sovellusten käytön ja uusien sovelluksien asentamisen päätelaitteeseen. Älypuhelimissa on usein avoin käyttöjärjestelmä, joka mahdollistaa uusien sovellusten asentamisen puhelimeen, jolloin puhelimen resurssit voidaan hyödyntää monipuolisesti. [50]

Älypuhelimissa käytetään osittain samoja käyttöjärjestelmiä, joita käytetään kämmentietokoneissa, kuten: Microsoft Windows Mobile 2003, Palm OS, Symbian OS. Myös muita laitevalmistajakohtaisia käyttöjärjestelmiä käytetään. [50]

5.5 Päätelaitteiden tietoturva

Käytettävät päätelaitteet voivat vaikuttaa merkittävästi koko VPN-ratkaisun tietoturvaominaisuuksiin, koska käyttöjärjestelmät ja laitteiden fyysiset ominaisuudet vaikuttavat mahdollisuuksiin käyttää eri ratkaisuja ja ohjelmistoja.

Päätelaitteen tietoturvaominaisuudet koostuvat päätelaitteessa käytetyn käyttöjärjestelmän tarjoamista tietoturvaominaisuuksista ja yhteensopivuudesta

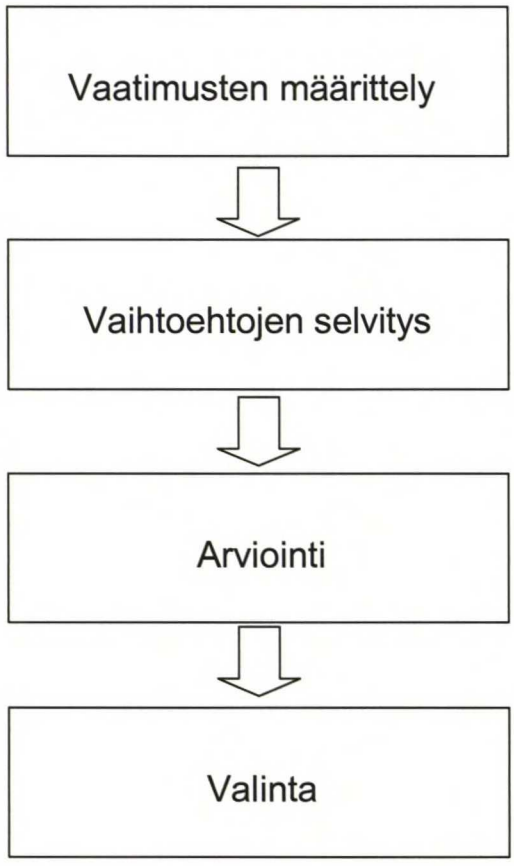
tietoturvaprotokollien kanssa. Lisäksi tietoturvaominaisuuksiin vaikuttavat päätelaitteeseen liitettävät lisälaitteet, kuten GPRS- tai WLAN-radiot tai lisälaitteina kiinnitettävät tunnistuslaitteet, kuten älykorttien lukijat. Päätelaitteen tietoturva ei siis ole riippuvainen suoranaisesti päätelaitteen tyypistä, vaan päätelaitteen liitäntämahdollisuuksista ja päätelaitteen käyttöjärjestelmän tietoturvaominaisuuksista.

Älypuhelimissa ja kämmentietokoneissa yleisimmin käytetyt käyttöjärjestelmät, kuten Microsoft Windows Mobile 2003, Palm OS ja Symbian OS tukevat VPN-ratkaisuiden käytön mahdollistavaa tietoturvaprotokollaa kuten IPsec tai PPTP [51,52,53]. Koska älypuhelimien käyttöjärjestelmät VPN-yhteyksissä käytettyjä tietoturvaprotokollia, on niille mahdollista toteuttaa VPN-asiakasohjelmistoja joita on jo saatavilla. [54] IPsec- tai PPTP-protokollia käyttävien asiakasohjelmistojen saatavuus älypuhelimille mahdollistaa samojen VPN-ratkaisuiden käytön sekä kannettavilla tietokoneilla että älypuhelimilla ja kämmentietokoneilla.

6 YRITYSVERKON MOBIILIYHTEYKSIEN ARVIOINTI

Arvioitaessa eri tapoja muodostaa langattomia yhteyksiä yrityksen tietoverkkoon, on huomioitava useita näkökulmia, jotka vaikuttavat yritysten tekemiin päätöksiin. Turvallisten järjestelmien ja yhteyksien suunnittelulla ei voida saavuttaa äärimmäistä turvallisuutta, eikä täydellistä käytettävyyttä, sillä kaikissa tapauksissa joudutaan tekemään kompromissi turvallisuuden ja käytettävyyden välillä. Pyrkimällä äärimmäiseen turvallisuuteen järjestelmä muodostuu käyttökelvottomaksi, mutta toisaalta järjestelmän suunnittelu käyttäjien ehdoilla saattaa johtaa tiedon ja tietoliikenteen luottamuksellisuuden vaarantumiseen alhaisten tietoturvakäytäntöjen johdosta. Sama logiikka pätee myös järjestelmän aiheuttamiin kustannuksiin, koska tietoturvan parantaminen tai käytettävyyden kehittäminen kasvattavat kustannuksia, mutta lisäävät samalla palvelun käytöllä saavutettavia hyötyjä.

Ratkaisuiden arviointiprosessi on monimutkainen, koska vaatimukset ja käytettävissä olevat resurssit vaihtelevat yrityskohtaisesti. Yrityskohtaisista vaatimuksista ja resursseista johtuen ratkaisuiden keskinäistä paremmuutta ei voida määritellä yleispätevästi eikä yksiselitteisesti. Tässä kappaleessa on asetettu joukko kriteerejä, joita voidaan käyttää eri ratkaisuiden arviointiin niitä hankkivan yrityksen näkökulmasta. Arvioinnin perusteella voidaan määritellä eri ratkaisuiden vahvuudet ja heikkoudet. Kappaleen lopussa käsitellään eri ratkaisuja tietoliikenneoperaattorin näkökulmasta.



Kuva 16 Mobiiliyhteysratkaisun valintaprosessi asiakasyrityksen kannalta

Kuvassa 16 on esitetty kaaviona prosessi, jonka mukaan mobiiliyhteysratkaisua hankkiva yritys voi edetä tarpeen havaitsemisesta ratkaisun käyttöönottoon. Ensimmäisessä vaiheessa yritys määrittelee ne tarpeet, joita täyttämään uutta ratkaisua ollaan hankkimassa. Määritellyistä tarpeista voidaan johtaa asetettavat vaatimukset, jotka toimivat arviointiprosessin lähtökohtana. Toisessa vaiheessa yritys selvittää ratkaisuja myyvien yritysten tarjoamia vaihtoehtoisia tuotteita, jotka ovat myöhemmin arvioinnin kohteena. Tässä vaiheessa kerätään lista tuotteista, jotka mahdollisesti täyttävät yrityksen asettamat vaatimukset. Kolmannessa vaiheessa yritys arvioi vaihtoehtoisia tuotteita omien vaatimustensa pohjalta käyttäen tiettyjä kriteerejä. Arvioinnin tuloksena saadaan selkeä kokonaiskuva eri ratkaisuiden soveltuvuudesta yrityksen tarpeisiin. Arviointi prosessi päättyy valintavaiheeseen, jossa yritys joko

valitsee yhden tai useampia ratkaisuja hankittavaksi tai päätyy lopputulokseen, jossa mikään tuotteista ei täytä asetettuja vaatimuksia. Jos mikään vaihtoehdoista ei täytä vaatimuksia, voidaan prosessia jatkaa alentamalla vaatimuksia ja tekemällä toinen arviointi uusiin vaatimuksiin pohjautuen.

6.1 Arvioinnissa käytetyt kriteerit

Yritysverkon mobiiliyhteyksien arviointi niitä käyttävän yrityksen kannalta voidaan jakaa kolmeen eri luokkaan, jotka ovat tietoturva, kustannukset ja yrityksen ja loppukäyttäjän kokema hyöty.

Kuva 17 Yrityksen mobiiliyhteysratkaisuiden arviointi

Kuvassa 17 esitetään, miten kolme näkökulmaa suhtautuvat toisiinsa ja erilaisiin mobiiliyhteysratkaisuihin. Kaikkia olemassa olevia ratkaisuja voidaan arvioida käyttäen näitä kolmea kriteeriluokkaa, jotka ovat keskenään vaihdannaisia. Tietoturvan tason parantaminen nostaa myös luultavasti kustannuksia ja voi vaikuttaa samalla

loppukäyttäjän kokemuksen laskemiseen. Myös kustannuksilla ja saavutetuilla eduilla on selkeä yhteys, koska panostamalla ratkaisuun taloudellisesti, saavutetaan enemmän hyötyjä yrityksen ja loppukäyttäjän kannalta.

6.1.1 Tietoturva

Vaikka yritysten tietoturva toteutetaan teknisillä ratkaisuilla, ovat yrityksen sisäiset tietoturvaprosessit merkittävä osa kokonaisvaltaista tietoturvaa. Tässä työssä on tarkoitus arvioida eri ratkaisuja mobiiliyhteyksien toteuttamiseksi, eikä ole tarkoitus käsitellä yrityksen sisäisiä prosesseja. Uuden ratkaisun käyttöönoton jälkeen on tärkeä määritellä prosessit, joiden mukaan tietoliikennepalveluita käytetään.

Ratkaisuiden teknistä tietoturvaa voidaan arvioida seuraavin kriteerein:

- Salatun yhteyden kattavuus
- Yhteyden suojauksen ja salauksen tehokkuus
- Käyttäjien autentikoitavuus ja pääsynhallinta.

Salatun yhteyden kattavuuden avulla tarkastellaan, mitkä osat koko yhteydestä on suojattu, ja missä osissa yhteyttä käyttäjä joutuu luottamaan ulkopuolisten verkkojen tietoturvaan ja verkkojen omistajaan välittäessään dataa kyseisissä verkoissa. Laajimmillaan salattu yhteys muodostetaan käytettävän päätelaitteen ja kohteena olevan palvelimen välille, jolloin välitettävä liikenne on suojattu koko yhteyden matkalta. Yhteyden suojaaminen päätelaitteen ja palvelimen välillä ei ole yritysten mobiiliyhteyksissä mielekästä, koska käyttäjät haluavat kommunikoida useiden yrityksen lähiverkossa olevien palvelimien kanssa. Tällöin salattu yhteys muodostetaan käyttäjän päätelaitteen ja yritysverkon ja julkisen verkon liityntäkohdassa olevaan yhdyskäytäväpalvelimen välille. Käytettäessä yhteyden suojausta ainoastaan tietyllä osalla koko yhteydestä, käyttäjien liikenne välitetään yrityksen ulkopuolisen tietoliikenneoperaattorin verkossa suojaamattomana. Tällöin yrityksen on luotettava

operaattorin verkon tarjoamiin tietoturvapalveluihin ja verkon turvallisuuteen. Mitä useampia välittäviä tahoja on, sitä suuremman riskin yritys ottaa käyttäessään kyseisiä yhteyksiä.

Yhteyden suojauksen ja salauksen tehokkuudella kuvataan ratkaisuissa käytettävien VPN-ohjelmistojen ja yhteyksien ja muiden tietoturva mekanismien tehokkuutta. Tämä tarkastelu koostuu useista eri tekijöistä, kuten käytetyistä protokollista, salausalgoritmeista ja käytetyistä laitteista ja verkoista.

Käyttäjien autentikoitavuus ja pääsynhallinta käsittelevät verkon toimintaa käyttäjien hallinnassa. Autentikoitavuudella ja pääsynhallinnalla kuvataan käytettävän ratkaisun kykyä erottaa käyttäjät toisistaan ja hallita käyttäjien oikeuksia yhteyksien ja verkon käyttöön.

6.1.2 Kustannukset

Kustannukset voidaan jakaa kahteen eri luokkaan:

- Järjestelmän aiheuttamat alkuinvestoinnit
- Järjestelmän käyttökustannukset

Mobiiliyhteysratkaisuja ostavat yrityksen näkökulmasta kustannukset jakautuvat kahteen eri luokkaan. Järjestelmän hankinnasta aiheutuu usein kertaluontoisia kustannuksia laite- ja ohjelmistohankinnoista. Lisäksi henkilökuntaa saatetaan joutua kouluttamaan uuden järjestelmän käytössä. Nämä kustannukset ovat järjestelmän hankinnasta aiheutuvia alkuinvestointeja.

Tietoliikennejärjestelmistä aiheutuu kustannuksia myös käyttöönoton jälkeen. Järjestelmän ylläpito, päivitys ja käyttäjien opastaminen aiheuttavat kustannuksia, jota arvioidaan järjestelmän käyttökustannuksina.

Järjestelmän aiheuttamat alkuinvestoinnit ja käyttökustannukset vaihtelevat ratkaisun arkkitehtuurista riippuen, joten niiden arviointi on kokonaisuuden kannalta tärkeää. Yritykset voivat toteuttaa langattomia yhteyksiä osittain itsenäisesti, ostaa järjestelmän omaan hallintaansa järjestelmätoimittajalta tai ostaa mobiiliyhteydet käyttöönsä kokonaispalveluna palveluntarjoajalta. Eri tavoilla toteutettujen ratkaisuiden kustannusrakenteet eroavat toisistaan merkittävästi. Itse rakennetuissa ratkaisuissa alkuinvestoinnit ovat suuret ja ylläpito saattaa aiheuttaa suuria kustannuseriä, jos ratkaisussa ilmenee ongelmia. Ostettaessa järjestelmä suoraan toimittajalta kustannukset koostuvat laitteiden ja ohjelmistojen hankinnasta ja itse suoritetusta järjestelmän ylläpidosta ja kehittämisestä. Ostettaessa koko palvelu operaattorilta saadaan verkko tai sen käyttöoikeus, ohjelmistot ja ylläpito samalta toimittajalta.

Kustannuksia arvioitaessa on mielenkiintoista käsitellä kiinteitä ja muuttuvia kustannuksia, eli tarkastella mitkä kustannukset ovat käyttäjien tai käyttöaktiivisuuden määrästä riippuvaisia ja mitkä eivät. Kustannuksia arvioitaessa on myös otettava huomioon, että vertailtavista verkoista ainoastaan langattomat lähiverkot soveltuvat yrityksen itsensä omistettavaksi.

6.1.3 Yrityksen ja loppukäyttäjän kokema hyöty

Yritykset hankkivat uusia tietoliikennepalveluita saavuttaakseen taloudellista hyötyä niiden avulla. Suoranaista taloudellista hyötyä on vaikea määrittää, joten on tärkeä arvioida minkä tyyppisiä hyötyjä yrityksen on mahdollista saavuttaa eri ratkaisuiden avulla. Yrityksen kokemat hyödyt eroavat usein varsinaisten loppukäyttäjien kokemista hyödyistä, joten niitä on arvioitava erikseen. Loppukäyttäjät ottavat uusia palveluita käyttöön, jos kokevat hyötyvänsä niiden käytöstä esimerkiksi työn helpottumisen tai joustavuuden lisääntymisenä.

Yrityksen ja loppukäyttäjän kokemaa hyötyä voidaan arvioida seuraavilla kriteereillä:

- Ratkaisun käyttömahdollisuuksien laajuus

- Ratkaisun tuomat edut yrityksen kannalta
- Ratkaisun tuomat edut yksittäisen käyttäjän kannalta.

Ratkaisun käyttömahdollisuuksien laajuudella kuvataan järjestelmän kykyä palvella käyttäjiä ajasta ja paikasta riippumatta. Käyttömahdollisuuksien laajuus riippuu käytettävien verkkojen peittoalueen laajuudesta ja tietoliikenneyhteyksien ja laitteiden toimintavarmuudesta.

Järjestelmän tuomat edut yrityksen kannalta ovat niitä konkreettisia syitä, joiden takia uusia ratkaisuja otetaan käyttöön. Yksittäisille käyttäjille näkyviä hyötyjä on mitattava taloudellista näkökulmaa abstrakteimmilla kriteereillä. Yrityksen mobiiliyhteysratkaisuilla on siis käyttäjiä kahdella eri tasolla, eli yrityksen tasolla ja yksittäisen käyttäjän tasolla. Yrityksen ja yksittäisten käyttäjien saavuttamat edut ovat osittain yhteneviä, mutta niissä on myös selviä eroja.

Yritysverkon mobiiliyhteyksien tarkoituksena on mahdollistaa työntekijöiden tehokas työskentely kiinteiden tietoliikenneverkkojen ulkopuolellakin. Työtekijät voivat liikkua yrityksen toimipisteiden sisällä, jolloin mobiiliyhteyksillä voidaan mahdollistaa liikkuville käyttäjille samat työskentelymahdollisuudet, jotka yrityksen lähiverkkoon kytketyillä päätelaitteilla työskennellessä saavutetaan. Työntekijät saattavat myös työskennellä yrityksen toimipisteiden ulkopuolella, jolloin mobiiliyhteyksillä voidaan hyödyntää lähiverkon palveluja sijainnista riippumatta. Mahdollistamalla työntekijöiden tehokas työskentely työntekijän sijainnista riippumatta, paranee työn tuottavuus ja näin saavutetaan myös yrityksen kannalta hyötyjä. Mobiiliyhteyden mahdollistavat lisäksi uusien työskentelykulttuurien syntymisen, koska niiden avulla työntekijä fyysinen sijainti ei välttämättä ole merkityksellistä tehtävän työn kannalta.

6.2 Arkkitehtuurivaihtoehtojen arviointi

Tässä työssä on esitelty seitsemän eri arkkitehtuuria, joiden mukaan yrityksen mobiiliyhteydet voidaan toteuttaa. Arkkitehtuurit on esitelty kappaleissa 5.1.1 ja 5.1.2 ja niiden ominaisuuksia on esitetty tiivistetysti taulukossa 2. Tässä taulukossa on esitetty ratkaisuiden tärkeimpiä ominaisuuksia, jolloin eri ratkaisuiden erot tulevat selvästi esille. Kappaleessa 6.1 on myös luotu kolmeen luokkaan jaetut kriteerit, joiden avulla eri arkkitehtuureja voidaan arvioida. Nämä luokat ovat tietoturva, kustannukset ja yrityksen ja loppukäyttäjän kokema hyöty. Tässä kappaleessa kriteerejä käytetään näiden seitsemän arkkitehtuurin arvioinnissa. Arkkitehtuurien arviointi on jaettu kolmeen kappaleeseen kriteerien luokittelun mukaisesti.

Taulukko 2 Yrityksen mobiiliyhteysratkaisuiden ominaisuudet

Arkkitehtuurit / Ominaisuudet		Internet-APN	VPN-APN	Yritys APN	WLAN Hot Spot	WLAN kodissa	WLAN Intranetin ulkopuolella	WLAN Intranetin sisäpuolella
Radioverkko	GPRS	X	X	X				
	WLAN				X	X	X	X
Käytetty suojaus	VPN	X			X	X	X	
	EI VPN		X	X				X
Verkon omistaja	Operaattori	X	X	X	X			
	Yritys					X	X	X
	Käyttäjä					X		
Autentikointitekniikka	SIM / HLR		X	X				X
	RADIUS	X			X	X	X	X
VPN-yhteyden hallinta	Yritys	X			X	X	X	X
	Ulkoistettu		X	X				X

6.2.1 Arkkitehtuurien arviointi tietoturvan kannalta

Tässä kappaleessa arkkitehtuurien arviointi on toteutettu kahdella taulukolla siten, että ensimmäisessä taulukossa on arvioitu pakettikytkentäisten matkapuhelinverkkojen käyttöön perustuvia ratkaisuja ja toisessa taulukossa langattomiin lähiverkkoihin perustuvia ratkaisuja. Molempien taulukoiden jälkeen on arviointia selvitetty jokaisen kriteerin kohdalta erikseen.

Taulukko 3 Pakettikytkentäisten matkapuhelinverkkojen käyttöön perustuvien VPN-ratkaisuiden arviointi tietoturvan kannalta

Arkkitehtuuri / Kriteeri	Yleinen GPRS-yhteys ja VPN-ohjelmisto	Operaattorin VPN-APN	Yrityskohtainen APN-osoite
Salatun yhteyden kattavuus	Yhteys suojattu päästä päähän	Yhteys suojattu VPN-ohjelmistolla ainoastaan osittain	
Tiedon suojauksen ja salauksen tehokkuus	Ominaisuuden riippuvat käytettävästä VPN-ohjelmistosta	Ominaisuudet operaattorin verkon ja käytettävän VPN-ohjelmiston mukaan	
Käyttäjien autentikointi ja pääsynhallinta	Autentikointimenetelmät riippuvat käytettävästä VPN-ohjelmistosta ja päätelaitteesta. Mahdollisuus käyttää vahvaa autentikointia	Käytössä laitepohjainen autentikointi ja yrityksen oma autentikointi	Mahdollisuus käyttää pelkkää laitepohjaista autentikointia. Voidaan käyttää myös yrityksen omia autentikointimenetelmiä

Taulukossa 3 on esitetty pakettikytkentäisten matkapuhelinverkkojen käyttöön perustuvien VPN-ratkaisuiden arvioinnin tulokset tietoturvan kannalta. Operaattorin VPN-APN ja yrityskohtainen APN-ratkaisut ovat samankaltaisia ja tietoturvan näkökulmasta nämä kaksi ratkaisua eroavat toisistaan ainoastaan käyttäjien tunnistamisen osalta.

Salatun yhteyden kattavuus

Yleiseen GPRS-yhteyteen perustuva ratkaisu koostuu matkapuhelinoperaattorin tarjoamasta suojaamattomasta ja langattomasta internetyhteydestä, sekä päätelaitteen ja yrityksen kotiverkossa sijaitsevan tietoturvayhdyskäytävän välille muodostettavasta

salatusta yhteydestä. Yhteys yritysverkon ja päätelaitteen välillä on siis salattu koko matkalla.

Operaattorin VPN-APN ratkaisuissa ja yrityskohtaista APN-osoitetta käytettäessä käyttäjien liikenne suojataan GPRS-radio- ja runkoverkoissa niiden omilla tietoturvamekanismeilla. Operaattorin ja ratkaisua käyttävän yrityksen verkoissa olevien VPN-keskittimien välillä liikenne on suojattu VPN-tunnelilla. Liikenne on siis suojattu VPN-tunnelilla ainoastaan osittain.

Tiedon suojauksen ja salauksen tehokkuus

Suojattaessa mobiiliyhteys erillisellä VPN-ohjelmistolla, riippuu tiedon luottamuksellisuus valitussa VPN-ohjelmistossa käytetystä protokollasta ja salausalgoritmista. Käytettäessä erillistä VPN-ohjelmistoa, voidaan se tarpeen vaatiessa päivittää uudempaan ilman koko arkkitehtuurin muuttamista, mikä on käyttäjän kannalta joustavaa.

Kahdessa ratkaisussa osa liikenteestä välitetään GPRS-verkossa, jota ei ole salattu VPN-yhteydellä, mutta siinä käytetään GPRS-verkon omia salausalgoritmeja radiotiellä. Suomessa operaattorien verkot ovat suljettuja ja siksi turvallisia välittäjäverkkoja, joten liikenteen välittäminen GPRS-verkossa ei muodosta merkittävää tietoturvariskiä mobiiliyhteyksiä käyttävälle yritykselle. Käytettäessä mobiiliyhteyttä ulkomailla, vierailevien verkkojen kautta, on kyseisten verkkojen turvallisuutta arvioitava tapauskohtaisesti. Näissä ratkaisuissa asiakas ei voi valita käytettävää VPN-ohjelmistoa, koska se on osa operaattorin kokonaisratkaisua.

Käyttäjien autentikointi ja pääsynhallinta

Koska yleiseen GPRS-yhteyteen perustuvassa arkkitehtuurissa VPN-yhteys muodostetaan erillisellä VPN-ohjelmistolla, voidaan käytettävä autentikointimenetelmä valita ohjelmiston tukemista menetelmistä. Useimmat VPN-ohjelmistot käyttävät käyttäjätunnukseen ja salasanaan perustuvia autentikointimenetelmiä, mutta haluttaessa

voidaan käyttää esimerkiksi toimikortteihin tai vaihtuviin salasanoihin tai jopa biometriseen tunnistukseen perustuvia menetelmiä. Mahdollisten autentikointimenetelmien määrää rajoittavat myös päätelaitteiden asettamat rajoitukset; kannettavaan tietokoneeseen on mahdollista asentaa ulkoisia tunnistuslaitteita, mutta yksinkertaisempien laitteiden kohdalla tämä ei välttämättä ole mahdollista.

Yrityskohtaisen ja VPN:lle dedikoitujen APN-osoitteiden käyttöön perustuvissa ratkaisuissa kyseisen osoitteen käyttöoikeus tarkistetaan käytettävän liittymän tiedoista matkapuhelinverkon tilaajatietokannasta. Yrityskohtaista APN-osoitetta käytettäessä käyttäjän liikenne ohjataan VPN-tunnelin kautta yrityksen verkossa olevan autentikointipalvelimen tunnistettavaksi. Tunnistamisessa voidaan käyttää esimerkiksi yrityksen RADIUS-palvelinta. Usean yrityksen käyttämässä VPN-käyttöön dedikoidussa APN-osoitteessa operaattorin on tunnistettava käyttäjät yrityskohtaisesti, eli määriteltävä, minkä yrityksen työntekijä on muodostamassa VPN-yhteyttä. Tämän tunnistuksen jälkeen käyttäjän liikenne ohjataan VPN-tunneliin ja käyttäjä autentikoidaan kuten yrityskohtaisen APN-osoitteen kohdalla. Matkapuhelinverkossa tapahtuva autentikointi ei ole tietoturvan kannalta ongelmallinen, koska palveluja käyttävä yritys käyttää lisäksi omia autentikointimenetelmiään.

Taulukko 4 Langattomien lähiverkkojen käyttöön perustuvien VPN-ratkaisuiden arviointi tietoturvan kannalta

Arkkitehtuuri / Kriteeri	WLAN- Hot Spot	WLAN kotona	WLAN intranetin ulkopuolella	WLAN Intranetin sisäpuolella
Salatun yhteyden kattavuus	Yhteys suojattu päästä päähän			Yhteys suojattu päätelaitteen ja liityntäpisteen välillä
Tiedon suojauksen ja salauksen tehokkuus	Luottamuksellisuus riippuu käytettävästä VPN-ohjelmistosta.		Luottamuksellisuus riippuu käytettävästä VPN-ohjelmistosta. Liikennettä ei välitetä ulkopuolisissa verkoissa	Luottamuksellisuus riippuu käytettävän WLAN-tekniikan salauksen vahvuudesta
Käyttäjien autentikointi ja pääsynhallinta	Autentikointimenetelmät riippuvat käytettävästä VPN-ohjelmistosta ja päätelaitteesta			Laitepohjainen autentikointi perustuu käytettävään WLAN-tekniikkaan

Salatun yhteyden kattavuus

Käytettäessä langattomia lähiverkkoja yrityksen mobiiliyhteyksien toteutuksessa, on suojattu yhteys kaikissa arkkitehtuureissa päästä-päähän yhteys, eli se kattaa koko yhteyden päätelaitteesta yritysverkkoon. Langattomissa lähiverkoissa käytetään siis VPN-yhteyttä tai muuta tietoturvamekanismia koko yhteydelle. Koska suojattu yhteys muodostetaan päätelaitteelta VPN-palvelimelle, ei ole tarpeellista arvioida liikennettä välittävien verkkojen tietoturvaa erikseen. Yhteyksien on oltava kaikissa langattomiin lähiverkkoihin perustuvissa ratkaisuissa näin kattavia, koska näissä verkoissa ei tarjota matkapuhelinverkkojen tapaan turvallisia kokonaisratkaisuja.

Tiedon suojauksen ja salauksen tehokkuus

Langattomiin lähiverkkoihin perustuvista arkkitehtuureista kolme perustuu erilliseen VPN-ohjelmistoon ja VPN-yhdyskäytäväpalvelimen käyttöön. Näiden arkkitehtuurien tiedon luottamuksellisuus riippuu käytettävän VPN-ohjelmiston algoritmeista ja protokollista. Käytettäessä VPN-yhteyttä langattomissa lähiverkoissa, on otettava

huomioon langattomien lähiverkkojen tietoturvauhat, kuten langattoman lähiverkon salauksen murtaminen, puskureiden ylivuotohyökkäykset ja liikenteen kaappaus. Langattomien lähiverkkojen tietoturvaa on käsitelty kappaleessa 4.3.1. Langattomia lähiverkkoja käytettäessä saatetaan tarvita VPN-ohjelmiston lisäksi päätelaitteisiin asennettavia palomuuriohjelmistoja riittävän tietoturvan takaamiseksi.

Intranetin sisäpuolelle liitettyyn langattomaan lähiverkkoon perustuvassa arkkitehtuurissa ei käytetä VPN-ohjelmistoa, vaan siinä langaton lähiverkko liitetään kiinteästi osaksi yrityksen lähiverkkoon. Tässä ratkaisussa tietoturva perustuu käytettävän WLAN-tekniikan tarjoamaan tietoturvaan. Kappaleessa 3.1 esitellyistä langattomien lähiverkkojen standardeista osa mahdollistaa tietoturvaominaisuuksien käytön. Laajimmin käytössä olevat 802.11b-standarin mukaiset verkot eivät tarjoa riittävää tietoturvaa, joten ne eivät sovellu tässä arkkitehtuurissa käytettäviksi. 802.11i- ja 802.11x-standardit tarjoavat tietoturvaominaisuuksia, joita voidaan ajatella käytettäviksi yritysverkoissa.[9]

Käyttäjien autentikointi ja pääsynhallinta

Maksullisissa Hot Spot-verkoissa käyttäjien tulee autentikoitua käyttäjätunnus ja salasana-parilla, joka valtuuttaa käyttäjän verkon käyttöön. Verkon käyttöoikeuden lisäksi käyttäjän tulee muodostaa VPN-yhteys yrityksen tietoverkkoon, jolloin käytettään yrityksen omia autentikointimenetelmiä.

Kuten pakettikytkentäisiä matkapuhelinverkkoja arvioitaessa todettiin, ei kaksinkertainen autentikointi välttämättä paranna ratkaisun turvallisuutta, vaan saattaa hankaloittaa palvelun käyttöä. Hot Spot-verkoissa tehtävän autentikoinnin tarkoitus on ainoastaan hallita verkon käyttöoikeuksia, eikä sillä ole merkitystä muodostettaessa yhteyttä yritysverkkoon.

Hot Spot-verkkojen lisäksi kaksi muuta langattomiin lähiverkkoihin perustuvaa arkkitehtuuria hyödyntää erillistä VPN-ohjelmistoa, joista useimmat tarjoavat

monipuoliset autentikointiominaisuudet. Näissä ratkaisuissa käytettävät autentikointitavat riippuvat ohjelmiston lisäksi päätelaitteen mahdollisuuksista.

Intranetiin suoraan yhdistetyssä langattomassa lähiverkossa ei voida suorittaa käyttäjien autentikointia, koska verkossa käytetään laitepohjaista autentikointia ja salausta. Laitepohjainen autentikointi saattaa olla turvallinen, mutta sen käyttö voi aiheuttaa ongelmia, koska verkon käyttäjiä ei kyetä tunnistamaan.

6.2.2 Arkkitehtuurivaihtoehtojen arviointi kustannusten kannalta

Taulukko 5 Yrityksen mobiiliyhteysratkaisuiden kustannusten vertailu

Arkkitehtuurit	Alkuinvestoinnit	Käyttökustannukset
Yleinen GPRS-yhteys ja VPN-ohjelmisto	GPRS-päätelaitteet, VPN-ohjelmistot ja laitteet	GPRS-käyttömaksut, Ohjelmistojen ja laitteiden ylläpito
Operaattorin VPN-APN	GPRS-päätelaitteet, operaattorin palvelun mukainen palvelun käyttöönottomaksu	GPRS-käyttömaksut, operaattorin hinnoittelun mukainen kuukausimaksu
Yrityskohtainen APN-osoite	GPRS-päätelaitteet, operaattorin palvelun mukainen palvelun käyttöönottomaksu	GPRS-käyttömaksut, operaattorin hinnoittelun mukainen kuukausimaksu
WLAN- Hot Spot	WLAN-kortit, VPN ohjelmistot ja laitteet	Hot Spot-palvelun käyttömaksut, VPN laitteiden ja ohjelmistojen ylläpito
WLAN kotona	WLAN-kortit, WLAN-tukiasemat, VPN-ohjelmistot ja laitteet	VPN-laitteiden ja ohjelmistojen ylläpito
WLAN intranetin ulkopuolella	WLAN-kortit, WLAN-verkko, VPN-ohjelmistot ja laitteet	Ohjelmistojen ja verkon ylläpito
WLAN Intranetin sisäpuolella	WLAN-kortit, WLAN-verkko	Verkon ylläpito

Kustannuksia arvioitaessa on mielenkiintoista tarkastella, miten käyttäjien ja käyttöaktiivisuuden määrä vaikuttaa eri kustannuselementteihin. Taulukossa 5 olevista kustannuksista GPRS-käyttömaksut ja Hot Spot-palveluiden käyttömaksut ovat puhtaasti muuttuvia kustannuksia, jotka kasvavat käyttäjä määrän ja käyttöaktiivisuuden kasvaessa. Päätelaitekustannukset, käyttäjämäärään perustuvat ohjelmistojen lisenssimaksut ja palvelumaksut ovat kustannuksia, jotka kasvat käyttäjämäärän

kasvaessa, mutta joihin käyttöaktiivisuuden muutos ei vaikuta. Muut kustannukset, kuten laitteiden hankintakustannukset ja ylläpitokustannukset ovat kiinteitä kustannuksia, joihin käyttäjien määrä ja käyttöaktiivisuus eivät merkittävästi vaikuta.

Alkuinvestoinnit ja käyttökustannukset pakettikytkentäisiin matkapuhelinverkkoihin perustuvissa ratkaisuissa

Yleiseen GPRS-yhteyteen perustuvassa arkkitehtuurissa GPRS-palvelu ja VPN-ohjelmistot ovat erillisiä komponentteja ja niistä aiheutuu vastaavasti erillisiä kustannuksia. Kahdessa muussa GPRS-verkkoa käyttävässä arkkitehtuurissa sekä GPRS-yhteys, että yhteyden suojauksessa käytetty VPN-palvelu ostetaan samalta operaattorilta, joka usein tarjoaa palvelua kokonaisratkaisuna. Kaikissa ratkaisuissa joudutaan investoimaan yhtäläisesti uusiin päätelaitteisiin.

GPRS-verkkoon perustuvissa ratkaisuissa asiakasyrityksen ei ole mahdollista omistaa käytettäviä matkapuhelinverkkoja, kuten langattomiin lähiverkkoihin perustuvissa ratkaisuissa voidaan tehdä. Tässä arvioinnissa ei kiinnitetä huomiota GPRS-palveluiden dataliikennemaksuihin ja niiden eroihin operaattori tai tuotekohtaisesti. Nämä maksut ja niiden vaihtelut ovat suhteellisen pieniä, eivätkä ne ole mielenkiintoisia tässä työssä tarkasteltavan kokonaisuuden kannalta.

Alkuinvestoinnit ja käyttökustannukset langattomiin lähiverkkoihin perustuvissa ratkaisuissa

Hot Spot- ja työntekijöiden kodeissa olevat langattomat lähiverkot eivät ole yrityksen hallinnassa, joten niiden käytöstä ei aiheudu kustannuksia samalla tavalla, kuin yrityksen omistamista verkoista. Näitä molempia verkkoja käytettäessä on yrityksellä oltava VPN-ohjelmistot ja palvelimet, joita luultavasti hyödynnetään muissakin yhteyksissä. Jos yrityksellä on jo tarvittavat VPN-ohjelmistot, on näiden kahden ratkaisun käyttöönotto suhteellisen edullista. Jos yrityksellä ei ole tarvittavia VPN-ohjelmia ja laitteita valmiina, on niiden hankkiminen kotona käyttävää langatonta lähiverkkoa tai Hot Spot-

palvelua varten kallista. Hot Spot-verkoista voidaan periä käyttömaksua, jotka vaihtelevat palveluntarjoajasta riippuen. Työntekijöiden kodeissa olevat verkot eivät ole yrityksen hallittavissa, joten voidaan ajatella, että niistä ei aiheudu käyttö- tai ylläpitokustannuksia yritykselle.

Yrityksen lähiverkkoon voidaan liittää langaton lähiverkko kahdella eri tavalla, jotka ovat kustannusten kannalta samantyyppisiä. Molemmissa vaihtoehdoissa yrityksen on hankittava itse tai ostettava palveluna langattoman lähiverkon laitteet omaan käyttöön. Itse verkon hankinnan lisäksi on oltava sopivat päätelaitteisiin liitettävät WLAN-kortit tai päätelaitteet, joissa on sopiva WLAN-radio. Liitettäessä langaton lähiverkko yrityksen lähiverkon ulkopuolelle, on verkon lisäksi hankittava suojatun yhteyden muodostamiseksi tarvittava VPN-palvelin ja VPN-asiakasohjelmat. Näiden kahden ratkaisun käytöstä aiheutuu WLAN-verkon ylläpitokustannuksia ja VPN-yhteyttä käyttävässä ratkaisussa ohjelmiston ja laitteiston ylläpitokustannuksia. Yrityksen verkon sisäpuolelle liitettävän verkon aiheuttamat alkuinvestoinnit voivat olla WLAN-verkon osalta ulkopuolelle liitettävää verkkoa suuremmat, koska joudutaan hankkimaan WLAN-verkon tietoturvaominaisuuksia tukevia laitteita.

6.2.3 Arkkitehtuurien arviointi yrityksen ja loppukäyttäjän kokeman hyödyn kannalta

Tässä kappaleessa esitetään, mitä hyötyjä yritys ja loppukäyttäjä kokevat käytettäessä eri arkkitehtuureja. Ensin käsitellään eri ratkaisuiden käyttömahdollisuuksien laajuutta, joka kuvaa järjestelmien kykyä palvella asiakkaita ajasta ja paikasta riippumatta. Käyttömahdollisuuksien laajuuden jälkeen käsitellään järjestelmien tuottamia hyötyjä ja heikkouksia sekä yrityksen että yksittäisen käyttäjän näkökulmasta.

Käyttömahdollisuuksien laajuus pakettikytkentäisiin matkapuhelinverkkoihin perustuvissa ratkaisuissa

Suomessa GPRS-verkko kattaa lähes koko maan ja samaa GPRS-yhteyttä voidaan käyttää myös ulkomailla operaattorien verkkovierailusopimusten nojalla. Verkkovierailun käyttö ei ole riippuvainen käytettävästä APN-osoitteesta, kuten kappaleessa 2.1.4 on esitetty, joten pakettikytkentäisiin matkapuhelinverkkoihin perustuvat ratkaisut eivät ero toisistaan tässä asiassa.

GPRS-yhteyksiin perustuvat yritysverkon mobiiliyhteydet ovat siis helposti käytettävissä sijainnista riippumatta ja niihin perustuvien ratkaisuiden käyttömahdollisuudet ovat laajat. Käyttömahdollisuuksiin vaikuttaa GPRS-verkon lisäksi VPN-palvelimien toimintavarmuus, eli mobiiliyhteydet yritysverkkoon toimivat ainoastaan, jos sekä GPRS-verkko että VPN-palvelimet toimivat. VPN-palvelimien luotettavuus on korkea ja niiden toimintaa voidaan valvoa ympärivuorokautisesti, jolloin mahdolliset toimintahäiriöt saadaan korjattua välittömästi.

Käyttömahdollisuuksien laajuus langattomiin lähiverkkoihin perustuvissa ratkaisuissa

Langattomat lähiverkot toimivat ainoastaan rajatuilla alueilla ja kaikki langattomat lähiverkot eivät ole ilmaisia tai julkisessa käytössä. Niillä alueilla, joilla langattomat lähiverkot toimivat, on niiden tarjoama tiedonsiirtoyhteys laajakaistainen ja laadukas. Käytettäessä langatonta lähiverkkoa esimerkiksi toimistoympäristössä, on sen toimivuus korkealla tasolla, koska WLAN-verkoilla pystytään kattamaan tehokkaasti sisätiloja. Tästä syystä langattomien lähiverkkojen kattavuus ei voi olla matkapuhelinverkkojen kattavuuden tasolla, eikä niitä ole mielekästä verrata toisiinsa.

Yrityksen kokemat hyödyt

Yleiseen GPRS-yhteyteen perustuvan arkkitehtuurin hyödyt ja haitat yrityksen kannalta:

+ Järjestelmä ei ole sidottu mihinkään mobiilioperaattoriin
+ Yhteys on salattu päästä päähän
+ Yritys voi valita VPN-järjestelmän toimittajan
– Yritys joutuu itse koordinoimaan palvelun ylläpitoa usean tahon kesken
– VPN-yhteyden aiheuttama lisäkuorma heikentää hyötysuhdetta radiorajapinnalla ja lisää tiedonsiirtokustannuksia
– Käyttäjät joutuvat käyttämään VPN-asiakasohjelmaa yhteydenmuodostuksessa

VPN-yhteyksille dedikoitu APN-arkkitehtuurin hyödyt ja haitat yrityksen kannalta:

+ Operaattori tarjoaa kokonaispalvelua
+ Ei tarvita erillistä asiakasohjelmistoa
– Sama palvelu on usean yrityksen käytettävissä
– Operaattori osallistuu käyttäjien autentikointiin
– Palvelu ei ole siirrettävissä operaattorilta toiselle

Yrityskohtaisen APN-ratkaisun hyödyt ja haitat:

+ Operaattori tarjoaa kokonaispalvelua
+ Ainoastaan yksi yritys käyttää kyseistä APN-osoitetta
– Palvelu ei ole siirrettävissä operaattorilta toiselle

WLAN Hot Spot:

+ Tarjoaa pienen lisän yrityksen käyttämien langattomien tietoliikenneyhteyksiin
+ Työntekijät voivat hyödyntää odotusaikaa esim. lentokentillä
- Monimutkaiset ja vaihtelevat hinnoittelumallit
- Madolliset tietoturvariskit

WLAN kotona:

+ Etätyöskentelyn tehostaminen mahdollista
- Saattaa aiheuttaa turvallisuusriskin
- Saattaa aiheuttaa ongelmia tietohallinnolle, jos käyttäjät joutuvat muokkaamaan päätelaitteiden asetuksia

WLAN intranetin ulkopuolella ja WLAN intranetin sisäpuolella:

+ Päätelaitteiden liikkuvuus työpaikan sisällä mahdollistaa tehokkaamman työskentelyn
+ Tietoverkon resurssit ovat käytettävissä langattoman verkon peittoalueella ja niitä voidaan hyödyntää joustavammin, kuin langallisissa lähiverkoissa
+ Mahdollisuus tarjota yrityksen vieraille langattomia verkkoyhteyksiä
+ Mahdollisuus säästää kiinteissä kaapeloinneissa käyttämällä langatonta lähiverkkoa
- Mahdolliset tietoturvariskit

Loppukäyttäjän kokemat hyödyt

Yleiseen GPRS-yhteyteen perustuvan arkkitehtuurin hyödyt ja haitat loppukäyttäjän kannalta:

+ Laajasti toimivat langattomat tietoliikenneyhteydet
+ VPN-ohjelmistoa voidaan käyttää myös muissa verkoissa
– Käyttäjältä vaaditaan VPN-yhteyden muodostuksessa toimenpiteitä
– Yhteyden kaistanleveys suhteellisen pieni
– VPN-yhteyden aiheuttama lisäkuorma heikentää hyötysuhdetta radiorajapinnalla, jolloin käyttäjän kokema tehollinen tiedonsiirtonopeus on teoreettista nopeutta alhaisempi

VPN-yhteyksille dedikoitu APN-arkkitehtuurin ja yrityskohtaisen APN-ratkaisun hyödyt ja haitat loppukäyttäjän kannalta:

+ Laajasti toimivat langattomat tietoliikenneyhteydet
+ Käyttäjältä ei vaadita monimutkaisia toimenpiteitä yhteyden muodostuksessa
+ Ei aiheuta lisäkuormaa radiorajapinnalla, joka vaikuttaa käyttäjän kokemaan tehollisen tiedonsiirtonopeuteen
– Yhteyden kaistanleveys suhteellisen pieni

WLAN Hot Spot:

+ Laadukkaat ja laajakaistaiset yhteydet
+ Soveltuu satunnaiseen käyttöön esim. lentokentillä, hotelleissa ja kongressikeskuksissa

- Maantieteellisesti rajalliset käyttömahdollisuudet
- Monimutkainen ja vaihtelevat hinnoittelumallit

WLAN kotona:

+ Laadukkaat ja laajakaistaiset yhteydet
+ Joustavat etätyöskentelymahdollisuudet
+ Mahdollisuus käyttää langatonta lähiverkkoa myös työn ulkopuolisiin tarkoituksiin

WLAN intranetin ulkopuolella ja WLAN intranetin sisäpuolella:

+ Laadukkaat ja laajakaistaiset yhteydet yrityksen toimipisteessä
+ Mahdollisuus työskennellä tehokkaasti langattoman verkon peittoalueella
+ Työskentelypisteen joustava muuttaminen

6.3 Tarkastelu tietoliikenneoperaattorin näkökulmasta

Tässä kappaleessa on tarkasteluyritysverkon mobiiliyhteyksiä niitä käyttävän yrityksen kannalta. Tietoliikenneratkaisuja tarkasteltaessa on mielenkiintoista ottaa huomioon myös asian toinen puoli, eli palveluja ja ratkaisuja tarjoavan tietoliikenneoperaattorin näkökulma. Tässä kappaleessa käsitellään, millä perusteella tietoliikenne operaattori voi arvioida eri mobiiliyhteysratkaisuja ja kuinka mielenkiintoisia eri ratkaisut ovat operaattorin kannalta.

Yritysverkon mobiiliyhteydet on mahdollista ottaa käyttöön yrityksen itsensä toteuttamana, ostaa ratkaisu osittain tai kokonaispalveluna operaattorilta. Tässä työssä käsiteltävistä verkoista ainoastaan yrityksen lähiverkkoon kytkettävä langaton lähiverkko soveltuu kokonaan yrityksen itsensä omistettavaksi, joten ratkaisuiden

tarkastelu operaattorin kannalta on mielenkiintoinen. Kaikki pakettikytkentäiset matkapuhelinverkot ovat operaattoreiden omistamia, mutta operaattori voi omistaa myös langattomia lähiverkkoja ja tarjota niitä palveluna yrityksille.

6.3.1 Operaattorin näkökulmien esittely

Tässä kappaleessa käsitellään tekijöitä, joiden perusteella operaattori arvioi eri ratkaisuja omasta näkökulmastaan. Operaattorin kannalta kiinnostavia näkökulmia ovat:

- Operaattorin rooli
- Operaattorilta vaadittavat toimenpiteet palvelun toimittamisessa
- Ratkaisuiden joustavuus ja muokattavuus.

Operaattorin roolilla kuvataan operaattorin asemaa asiakasyrityksen ostaessa tietoliikennepalveluja. Palvelua tarjoavalla operaattorilla voi olla erilaisia rooleja ja roolista riippuen erilaisia velvollisuuksia ja mahdollisuuksia. Alhaisimmillaan operaattorin rooli on silloin, kun se tarjoaa ainoastaan tiedonsiirtokapasiteettia yrityksen käyttöön ja sitä merkittävämpi se on, mitä kattavampaa palvelua asiakas operaattorilta ostaa. Suurin operaattorin rooli on silloin, kun se tarjoaa pelkän tiedonsiirtokapasiteetin sijaan kokonaisratkaisun mobiiliyhteyksien toteuttamiseksi.

Operaattorilta vaadittavilla toimenpiteillä arvioidaan operaattorin tekemän työn määrää ratkaisua toimitettaessa. Operaattori toimittaa asiakkailleen sopimusten mukaisia laitteita ja palveluita, jolloin sen roolista ja toimitettavasta tuotteesta tai palvelusta riippuen sillä on erilaisia tehtäviä. Operaattori saattaa toimia ainoastaan laitteiden myyjänä, jolloin tehtävät rajoittuva laitteiden toimittamiseen. Myytäessä asiakkaalle kokonaisvaltaisempia ratkaisuja, saatetaan tarvita laitteiden toimittamisen lisäksi esimerkiksi muutoksia tietokantoihin tai uusien ohjelmistojen asennuksia.

Ratkaisun muokattavuudella tarkoitetaan operaattorin mahdollisuuksia muuttaa käytössä olevaa palvelua heikentämättä asiakkaiden kokemaa palvelunlaatua. Joustavuudella tarkoitetaan mahdollisuuksia muokata ratkaisua asiakkaan toiveiden mukaisesti. Operaattorit haluavat tarjota asiakkailleen mahdollisimman hyvää palvelua, jolloin palvelun kehittämismahdollisuudet on otettava huomioon eri vaihtoehtoja arvioitaessa.

6.3.2 Arkkitehtuurien arviointi operaattorin kannalta

Operaattorin kannalta pakettikytkentäisen matkapuhelinverkot ja langattomat lähiverkot eroavat toisistaan merkittävästi, joten niitä on mielekästä tarkastella erillisinä joukkoina. Pakettikytkentäiset matkapuhelinverkot ovat poikkeuksetta operaattorin omistuksessa ja operaattori tarjoaa tietoliikennepalveluita kaikille asiakkailleen. Langattomiin lähiverkkoihin perustuvien VPN-arkkitehtuureiden arviointi operaattorin kannalta ei ole samalla tavalla suoraviivaista kuten matkapuhelinverkkoihin perustuvissa arkkitehtuureissa, koska ratkaisuissa operaattoreiden osuudet vaihtelevat suuresti ja toimijoina voi olla useita eri operaattoreita. Lisäksi langattomissa lähiverkoissa käytettävät laskutusmallit eroavat suuresti matkapuhelinverkkojen pakettikytkentäisen liikenteen hinnoittelusta.

Tässä kappaleessa käsitellään ensin pakettikytkentäisiin matkapuhelinverkkoihin perustuvia arkkitehtuurit ja niiden jälkeen langattomiin lähiverkkoihin perustuvat arkkitehtuurit. Molempien osien alussa arviointi on tiivistetty taulukoiksi, joissa eri arkkitehtuureita on arvioitu kolmen eri kriteerin kannalta. Taulukoiden jälkeen arviointia on selvennetty kriteereittäin.

Taulukko 6 Pakettikytkentäisten matkapuhelinverkkojen käyttöön perustuvien VPN-arkkitehtuureiden arviointi operaattorin kannalta

Arkkitehtuuri / Kriteeri	Yleinen GPRS-yhteys ja VPN-ohjelmisto	Operaattorin VPN-APN	Yrityskohtainen APN-osoite
Operaattorin rooli	Alhainen, jos toimitetaan pelkkä GPRS-yhteys	Merkittävä, koska toimitetaan kokonaisratkaisu	
Operaattorilta vaadittavat toimenpiteet palvelun toimittamisessa	GPRS-peruspalvelu ja mahdollisten VPN-laitteiden toimitus	GPRS-palvelu, muutokset verkon tietokantoihin, palvelimen hankinta asiakkaalle	GPRS-palvelu, muutokset verkon tietokantoihin, APN-osoitteen luominen, palvelimen hankinta asiakkaalle
Ratkaisuiden joustavuus ja muokattavuus	Mahdollista muokata VPN-ohjelmistoa muuttamalla tai vaihtamalla	Hankala muokata, koska usea yritys käyttää samaa palvelua	Mahdollista muokata autentikointimenetelmiä, laskutusmalleja

Operaattorin rooli

Yleiseen GPRS-palveluun perustuvassa ratkaisussa operaattorin rooli on muihin ratkaisuihin verrattuna pienin. Tässä ratkaisussa operaattorilta ostetaan vähintään GPRS-palvelu, joka on operaattorin peruspalvelu, eikä se sido asiakasta tietyn operaattorin asiakkaaksi. Vaikka yritykselle, myytäisiin GPRS-palvelun lisäksi VPN-laitteet ja ohjelmistot, ei asiakas ole silti sidoksissa operaattoriin.

Kaksi muuta ratkaisua perustuvat operaattorin tarjoamaan kokonaispalveluun, jossa asiakkaan käyttämä palvelu on saatavissa sellaisenaan ainoastaan kyseiseltä operaattorilta ja operaattorin vaihtaminen edellyttää uuden palvelun ostamista uudelta operaattorilta. Näissä ratkaisuissa operaattorin rooli on korkea ja sekä asiakas että operaattori ovat sitoutuneet kyseiseen asiakassuhteeseen.

Operaattorilta vaadittavat toimenpiteet palvelun toimittamisessa

Yleiseen GPRS-yhteyteen perustuvissa ratkaisuissa käyttäjät ostavat operaattorilta GPRS-peruspalvelun, jota käytetään VPN-ohjelmistojen ja laitteiden kanssa

yritysverkon mobiiliyhteyksien muodostamisessa. Operaattorille tämän ratkaisun myyminen ei eroa normaalista liittymien tai lisäpalveluiden myymisestä, eikä siis aiheuta välittömiä kustannuksia. Tässä arkkitehtuurissa VPN-palvelin sijaitsee yrityksen verkossa, joten vaikka operaattori toimittaisi myös tämän palvelimen, ei operaattorin verkkoon tarvita muutoksia.

Yrityskohtaisella APN:llä toteutetun VPN-ratkaisun käyttöönotossa operaattori muodostaa uuden APN-osoitteen ja sallii kyseisen osoitteen käytön asiakkaan liittymillä. VPN-käyttöön tarkoitettua APN-osoitetta käytettäessä ei tarvita uutta APN-osoitetta jokaista uutta asiakasta kohti. Palvelun käyttöönotto vaatii verkkoon tehtävien muutosten lisäksi asetusten muuttamista käyttäjien päätelaitteisiin ja VPN-yhdyskäytävän asentamista asiakkaan lähiverkkoon. Usein operaattori suosittelee hankittavaksi tiettyä laitetta tai toimittaa laitteen suoraan asiakkaalle.

Ratkaisun joustavuus ja muokattavuus

Yleiseen GPRS-yhteyteen perustuva ratkaisu käyttää mobiilioperaattorin perustuotetta: yleistä GPRS-yhteyttä, jolla on paljon erilaisia käyttäjiä. Koska yleinen GPRS-yhteys on operaattorin perustuote, jota asiakkaat voivat käyttää haluamiinsa tarkoituksiin, ei sitä ole tarkoitus räätälöidä asiakkaan tarpeiden mukaan. Tässä ratkaisussa räätälöintiä voidaan mahdollisesti tehdä VPN-ohjelmiston tarjoamien mahdollisuuksien puitteissa tai vaihtamalla käytettävää VPN-ohjelmistoa.

Yrityskohtaiseen APN-osoitteeseen perustuva ratkaisu on ainoastaan asiakasyrityksen käytössä ja jokaista uutta asiakasta kohden perustetaan uusi APN-osoite. Operaattori käyttää kuitenkin kaikilla asiakkailla samaa VPN-yhdyskäytävää, joten palvelu ei ole täysin asiakaskohtainen. Tässä ratkaisussa operaattorilla on mahdollisuus tarjota yksilöllistä palvelua muuttamalla APN-osoitteen toimintaa, jolla voidaan vaikuttaa autentikointimenetelmiin ja käytettäviin laskutusmalleihin.

Operaattorin VPN-APN arkkitehtuuri on muunneltavuuden kannalta kahden edellisen arkkitehtuurin välimuoto. VPN-APN ratkaisu on tarkoitettu useamman yrityksen käytettäväksi, joten palvelua ei voida muokata yhden asiakkaan toiveesta, kuten yrityskohtaisessa ratkaisussa voidaan tehdä. Tämä ratkaisu onkin muokattavuudeltaan kolmesta GPRS-yhteyttä käyttävästä ratkaisusta heikoin, koska sitä ei voida muokata APN-osoitteen, eikä VPN-ohjelmiston avulla.

Taulukko 7 Langattomien lähiverkkojen käyttöön perustuvien VPN-ratkaisuiden arviointi operaattorin kannalta

Arkkitehtuuri / Kriteeri	WLAN- Hot Spot	WLAN kotona	WLAN intranetin ulkopuolella	WLAN Intranetin sisäpuolella
Operaattorin rooli	Ei merkittävää roolia		Operaattori voi toimittaa kokonaisratkaisun tai ainoastaan osia siitä. Operaattori voi ylläpitää ratkaisua	Operaattori voi toimittaa verkon käyttövalmiina ja ylläpitää sitä
Operaattorilta vaadittavat toimenpiteet palvelun toimittamisessa	Ei toimenpiteitä verkkoon tai VPN-ohjelmistoon liittyen		Operaattori toimii kokonaisratkaisun tarjoajana, jolloin tehtävät voivat olla hyvinkin laajat	
Ratkaisuiden joustavuus ja muokattavuus	Muokattavuus VPN-ohjelmiston kautta. Verkkopalvelu ei muokattavissa	Muokattavissa VPN-ohjelmiston kautta. Verkko käyttäjän hallinnassa	Ratkaisu ainoastaan asiakasyrityksen käytössä, joten se on helposti muokattavissa	Ratkaisu ainoastaan asiakasyrityksen käytössä, joten se on helposti muokattavissa

Operaattorin rooli

Sekä Hot Spot-verkkoihin että kodeissa käytettäviin langattomiin lähiverkkoihin perustuvissa ratkaisuissa verkko-operaattorit toimivat ainoastaan tietoliikenneyhteyden tarjoajina, joten niiden rooli on pieni kokonaisuuden kannalta.

Yrityksen lähiverkkoon liitettävissä ratkaisuissa operaattori toimii usein merkittävässä roolissa langattomien lähiverkkojen kokonaispalvelujen toimittajana. Yrityksen

lähiverkkoihin liitettävät langattomat lähiverkot voivat olla joko yrityksen itsensä rakentamia ja ylläpitämiä tai ne on voitu ostaa palveluna esimerkiksi lähiverkkoa ylläpitävältä ja Internet-yhteyksiä tarjoavalta operaattorilta. Näissä ratkaisuissa operaattorin rooli voi korostua operaattorin toimiessa tietoturvan asiantuntijana asiakkaan suuntaan.

Operaattorilta vaadittavat toimenpiteet palvelun toimittamisessa

Hot Spot-verkkoja hyödyntävässä arkkitehtuurissa verkko ja siinä käytettävä VPN-yhteys eivät ole sidoksissa toisiinsa, eikä näiden verkkojen käyttö vaadi palvelua myyvältä taholta mitään toimenpiteitä. Kodeissa olevat verkot ovat usein työntekijöiden yksityisomaisuutta, eikä yrityksellä tai verkko-operaattorilla ole mitään siteitä näihin verkkoihin. Näiden verkkojen käyttö yrityksen mobiiliyhteyksissä ei myöskään vaadi toimenpiteitä operaattorilta. Näissä kahdessa arkkitehtuurissa käytetään VPN-ohjelmistoa, jonka pääasiallinen käyttötarkoitus ei liity suoranaisesti näihin verkkoihin, joten myöskään ohjelmiston toimittajalta ei vaadita toimenpiteitä kyseisiin verkkoihin liittyen.

Kaksi muuta langattomia lähiverkkoja käyttävää arkkitehtuuria on tarkoitettu ainoastaan asiakasyrityksen käyttöön, jolloin operaattorin tehtävänä on toimittaa toimivat verkot ja ohjelmistot asiakkaalle. Näitä verkkoja toimitettaessa operaattorin tehtävät voivat olla hyvinkin laajat riippuen asiakkaan ostaman palvelun kattavuudesta ja laajuudesta.

Ratkaisun joustavuus ja muokattavuus

Arvioitaessa langattomia lähiverkkoja käyttäviä VPN-ratkaisuja niiden joustavuuden ja muokattavuuden kannalta, on otettava huomioon operaattorin rooli kussakin ratkaisussa. Hot Spot-verkot ovat usein VPN-ratkaisuista täysin erillinen palvelu varsinkin silloin kun niitä tarjoava taho ei ole tekemisissä VPN-ratkaisuiden kanssa. Operaattorin roolin pienuuden ja Hot Spot-verkkojen laajan käyttäjäkunnan takia näiden verkkojen muokattavuus ja joustavuus ovat alhaisella tasolla.

Työntekijöiden kodeissa olevat verkot ovat Hot Spot-verkkoja huomattavasti joustavampia. Vaikka VPN-ratkaisua hallinnoivalla yrityksellä ei ole mahdollisuuksia vaikuttaa kodeissa oleviin langattomiin lähiverkkoihin, voivat käyttäjät kuitenkin itse muokata niitä omien tarpeidensa mukaan ja saada ne toimimaan joustavasti käytettävien VPN-ratkaisuiden kanssa.

Yrityksen lähiverkkoon liitettävien langattomien lähiverkkojen on täytettävä ainoastaan niitä käyttävän yrityksen tarpeet, jolloin niihin voidaan tehdä muutoksia ja parannuksia tarvittaessa. Yrityksen lähiverkon ulkopuolelle sijoitettu langaton lähiverkko koostuu itse verkosta ja VPN-ohjelmistoista, joten sitä ratkaisua voidaan parantaa päivittämällä joko verkkoa tai VPN-ohjelmistoa. Suoraan yrityksen lähiverkkoon kytketyssä ratkaisussa verkon tietoturva on sidottu käytettäviin laitteisiin, joten myös tietoturvaa parannettaessa voidaan joutua vaihtamaan verkon laitteita. Verkon laitteiden mahdollinen vaihtotarve johtuu langattomien lähiverkkojen standardeista, joiden uusia tietoturvaominaisuuksia ei välttämättä voida ottaa käyttöön vanhoissa laitteissa.

7 JOHTOPÄÄTÖKSET

Työn ensisijaisena tavoitteena oli luoda joukko kriteerejä, joiden perusteella yritysverkon mobiiliyhteyksiä voidaan arvioida. Työn toisena tavoitteena oli arvioida määriteltyjä arkkitehtuurivaihtoehtoja luotujen kriteerien perusteella ja näin esitellä eri arkkitehtuurien vahvuudet ja käyttökelpoisuus erilaisiin tarkoituksiin yritysverkoissa.

Työssä luotiin joukko kriteerejä, jotka tarkastelevat yritysverkon mobiiliyhteyksiä kolmesta eri näkökulmasta. Koska mobiiliyhteydet kulkevat usein yrityksen ulkopuolisten tai muuten haavoittuvien verkkojen kautta, on ratkaisuiden tietoturvan arviointi ensiarvoisen tärkeää. Ratkaisuiden tietoturvaa arvioitiin neljää eri kriteeriä käyttäen. Yrityksen tietoliikenneratkaisut ovat merkittävä osa tietotekniikkaympäristöä, joten asiakasyrityksen vaatimusten arvioimiseksi luotiin myös neljä kriteeriä. Yritykset eivät yleensä voi tai halua toteuttaa langattomia tietoliikenneyhteyksiään itse, vaan kyseiset palvelut ostetaan ulkopuoliselta tietoliikenneoperaattorilta. Kolmas näkökulma, jonka perusteella ratkaisuja arvioitiin, oli yritysverkon mobiiliyhteyksiä tarjoavan operaattorin näkökulma. Operaattorin näkökulman arvioimiseksi määriteltiin kolme kriteeriä.

Luotujen kriteerien avulla pystytään arvioimaan tehokkaasti erilaisia ratkaisuja usealta eri kannalta. Kriteerejä voidaan käyttää tässä työssä tehtyä arviointia huomattavasti tehokkaammin todellisia ratkaisuja arvioitaessa. Tässä työssä arvioidut seitsemän arkkitehtuuria ovat malleja, joihin todelliset ratkaisut perustuvat, eikä niiden arviointi vastaa todellisten ratkaisuiden arviointia malleissa olevien vaihtoehtoisten toteutustapojen takia. Todellisissa ratkaisuissa toteutusvaihtoehdoista on valittu yksi ja arviointi voidaan siksi tehdä mallin arviointia tarkemmin.

7.1 Arvioinnin tulokset

Yleiseen GPRS-yhteyteen perustuvasta ratkaisusta voidaan todeta, että se on tietoturvan kannalta kattava ratkaisu, joka soveltuu hyvin yrityskäyttöön. Tämä ratkaisu ei sido asiakasta kiinteästi operaattoriin, sillä käytettävä GPRS-yhteys on vaihdettavissa kilpailevan operaattorin vastaavaan palveluun ja VPN-ohjelmisto voidaan myös vaihtaa tarvittaessa. Operaattorin kannalta tämä ratkaisu on helppo toteuttaa, koska verkkoon tehtävät muutokset ovat vähäisiä. Ratkaisu ei tosin välttämättä ole operaattorin kannalta kiinnostava, koska asiakasta on vaikea sitouttaa.

Operaattorin VPN-APN-osoitetta käyttävä ratkaisu voi olla operaattorin kannalta ongelmallinen, koska tässä ratkaisussa joudutaan käyttämään muita ratkaisuja monimutkaisempia autentikointimenetelmiä GPRS-verkossa. Muuten tämä ratkaisu on operaattorin kannalta vaivaton, koska uusien asiakkaiden aiheuttamat toimenpiteet ovat suhteellisen pieniä. Asiakkaan kannalta tämä ratkaisu ei mahdollista joustavaa palvelua, koska samaa ratkaisua käyttävät useat yritykset, eikä operaattorilla ole mahdollisuuksia räätälöidä palvelua yksittäisen asiakkaan toivomuksien mukaan.

Yrityskohtaiseen VPN-osoitteeseen perustuva ratkaisu on asiakkaan näkökulmasta parhaiten räätälöity palvelu. Tässä arkkitehtuurissa asiakkaalle tarjotaan oma APN-osoite käyttöön, jolloin käyttö on helppoa ja osoitteen käyttäjinä on ainoastaan yhden yrityksen henkilökuntaa. Operaattorin kannalta tämä ratkaisu on mielenkiintoinen, koska asiakas on hyvin sitoutunut ja operaattorin vaihtaminen olisi asiakkaan kannalta monimutkaista. Koska tähän ratkaisuun perustuva palvelu on asiakaskohtaista, on operaattorilla mahdollisuus tarjota monipuolisia vaihtoehtoja palvelun toiminnassa.

Hot Spot-verkkoihin ja kodeissa oleviin verkkoihin perustuvat ratkaisut eroavat muista työssä esitetyistä ratkaisuista merkittävästi, koska näitä ratkaisuja käytetään joko satunnaisesti tai työntekijöiden oman aktiivisuuden ansiosta. Nämä ratkaisut eivät siis tarjoa yrityksille monipuolista kokonaisratkaisua, vaan ainoastaan täydentävät muita käytössä olevia ratkaisuja. Koska nämä verkot eivät ole operaattorin hallinnassa ja

verkoilla voi olla muitakin käyttäjiä, on päätelaitteiden ja yhteyksien tietoturvaan kiinnitettävä erityisesti huomiota. Yrityksen mobiiliyhteyksiä tarjoavan operaattorin kannalta nämä ratkaisut eivät ole mielenkiintoisia, koska ratkaisuihin on hankala yhdistää sopivia tietoturvapalveluita ja ratkaisuja on hankala myydä yrityksille kattavana palveluna.

Intranetin ulkopuolelle liitettävä langaton lähiverkko on asiakasyrityksen kannalta läpinäkyvä ratkaisu, jossa olemassa olevan lähiverkon toimintaa laajennetaan saumattomasti. Läpinäkyvyyden kustannuksella verkon tietoturvassa saattaa olla puutteita, joita voi olla hankala parantaa ja samalla verkon päivittäminen voi olla työlästä. Tämän ratkaisun käyttö vaatii syvällistä tietoturvaosaamista, jota operaattori voi asiakkailleen tarjota. Tästä johtuen kyseinen ratkaisu on operaattorin kannalta houkutteleva tuotevaihtoehto.

Intranetin ulkopuolelle sijoitettava langaton lähiverkko on käyttäjien kannalta suoraan intranettiin liitettäviä verkkoja monimutkaisempi siinä käytettävien VPN-ohjelmistojen takia. Toisaalta VPN-ohjelmistot mahdollistavat korkean tietoturvan tason ja yrityksen tietoturvavaatimusten mukaisten menetelmien käytön. Lisäksi tämän arkkitehtuurin käyttö mahdollistaa VPN-ohjelmiston käytön muissakin yhteyksissä, kuten Hot Spot-verkoissa ja käyttäjien kodeissa. Operaattorin kannalta tämä ratkaisu on kiinnostava, koska se tarjoaa mahdollisuuden toimia merkittävässä roolissa kokonaispalvelun tarjoajana.

Arvioinnin perusteella voidaan todeta, että mikään esitetyistä arkkitehtuureista ei tarjoa yleispätevää ratkaisua, jolla voitaisiin toteuttaa kaikkien yritysten mobiiliyhteydet. Luotuihin kriteereihin perustuva arviointi ei anna yksikäsitteisiä vastauksia eri arkkitehtuurien paremmuudesta, vaan määrittelee perusteet, joiden mukaan niitä voidaan arvioida. Luotuja arviointikriteerejä voidaan parhaiten hyödyntää painottamalla arviointiprosessia sitä suorittavan tahon tarpeiden ja vaatimusten mukaan. Yritysverkkonsa mobiiliyhteyksiä suunnittelevaa yritystä kiinnostaa eri ratkaisuiden

tietoturva ja ratkaisuiden arviointi omasta näkökulmastaan. Yrityksen suorittaessa valintaprosessia on työ tehtävä järjestelmällisesti. Yrityksen on määriteltävä ratkaisulle asetettavat vaatimukset, selvitettävä vaihtoehtoiset tuotteet ja arvioitava niitä vaatimusten ja arviointikriteerien avulla. Tietoliikenneoperaattori puolestaan voi arvioida eri vaihtoehtoja tarkoituksenaan tuotteistaan yksi tai useampi ratkaisu ja myydä niitä asiakkailleen. Tällöin operaattori on luultavasti kiinnostunut kaikista tässä työssä määritellyistä kriteereistä, mutta varmastikin eri tavalla kuin palveluja ostava asiakasyritys. Operaattori voi myös hyödyntää luotuja kriteerejä olemassa olevien tuotteiden arvioinnissa ja etsiä mahdollisia kehityskohteita.

7.2 Jatkotutkimukset

Matkapuhelinverkkojen kehittyminen ja kolmannen sukupolven verkkojen valmistuminen mahdollistavat nykyistä tehokkaammat mobiiliyhteydet yrityksen tietoverkkoihin. Tämä kehitys avaa myös uusia mahdollisuuksia yritysverkkojen mobiiliyhteyksissä käytettäville ratkaisuille ja saattaa antaa aihetta tutkimusten jatkamiselle. Kolmannen sukupolven matkapuhelinverkkoihin yhdistetty All-IP ajattelu ja liikenteen palvelunlaatu-luokat, joiden avulla operaattorit voivat erilaistaa palveluitaan, vaikuttavat myös yritysten mobiiliyhteyksiin. Nämä kolmannen sukupolven matkapuhelinverkkojen ominaisuudet ovat mielenkiintoisia tarkastelukohteita tulevaisuudessa.

Mobiiliverkoissa käytettävät päätelaitteet kehittyvät jatkuvasti ja varsinkin älypuhelimien kehitystä on syytä seurata mielenkiinnolla. Uudet päätelaitteet saattavat parantaa yritysverkon mobiiliyhteyksien käyttömahdollisuuksia ja lisätä samalla näiden ratkaisuiden merkitystä asiakasyritysten ja operaattoreiden kannalta.

Matkapuhelinverkkojen ja langattomien lähiverkkojen välisen verkkovierailun toteutuminen tulevaisuudessa mahdollistaa useiden erilaisten verkkojen käytön yhdellä

päätelaitteella joustavasti ja saumattomasti. Tämä kehitys voi olla edistämässä myös osaltaan yritysverkkojen mobiiliyhteyksien käyttöä.

Tässä työssä arvioitiin yksittäisiä arkkitehtuureja useilta eri näkökulmilta. Tätä työtä voidaan jatkaa selvittämällä laajempia, useista eri ratkaisuista muodostuvia kokonaisuuksia, joissa yrityksen mobiiliyhteyksien toteuttamisessa käytetään tehokkaasti erilaisia verkkoja ja ratkaisuja. Näiden jatkotutkimusten perusteella voivat yritykset hahmottaa sirpaleisen palvelukentän kiinteämpänä kokonaisuutena ja tietoliikennealalla laajasti toimivat operaattorit voivat muodostaa yksittäisistä tuotteistaan mielekkäitä tuotekokonaisuuksia.

LÄHTEET

[1] Radiolinja Oy. 2003. GPRS-palvelun käyttö ulkomailla. [viitattu 22.9.2003]. https://www.radiolinja.fi/go?section=tuotteet_ja_palvelut/liittyman_palvelut/gprs_lisapalvelu&page=gprs_roaming

[2] Järvinen, H. 2003. WLAN vie langattomaan internetiin, Pääkirjoitus. Tietokonelehti 6-7/2003.

[3] Anderson, R. 2001. Security Engineering: A Guide to Building Dependable Distributed Systems. New York, United States of America. Wiley Computer Publishing. 612 p. ISBN 0471 38922-6

[4] Shneyderman, A.; Casati, A. 2003. Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems. United States of America. Wiley Publishing, Inc. 330 p. ISBN 0471 21901 0.

[5] Penttinen, J. 2001. GSM-tekniikka; Järjestelmän toiminta ja kehitys kohti UMTS-aikakautta Helsinki. WSOY 412 s. ISBN 9510 26038 X

[6] Penttinen, J. 2001. GPRS-tekniikka; Verkon rakenne, toiminta ja mitoitus. Helsinki. WSOY. 264 s. ISBN 9510 26558 6.

[7] Radiolinja Suomi Oy. 2003. Yrityshinnasto. 13 p. [viitattu 15.9.2003]. https://www.radiolinja.fi/common_documents/fi/pdf/Yrityshinnasto_su.pdf

[8] 3GPP TS 23.060 V3.15.0. 2003. Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2 (Release 1999). 3rd Generation Partnership Project. 193 p.

[9] Kaaranen, H.; Ahtiainen, A.; Laitinen, L.; Naghian, S.; Nieminen, V. 2001. UMTS Networks; Architecture, Mobility and Services. Chichester, England. John Wiley & Sons, LTD. 302 s. ISBN 047148543 X.

[10] 3GPP TS 23.03 V5.6.0. 2003. Technical Specification Group Core Network; Numbering, addressing and identification; (Release 5). 3rd Generation Partnership Project. 39 p.

[11] Hoffman, J. editor. 2003. GPRS demystified. New York, United States of America. McGraw-Hill. 457 p. ISBN 007 138553 3.

[12] Nokia Corporation. 2003. GSM/GPRS/EDGE. [viitattu 23.4.2003]. http://www.nokia.com/cda1/0,1080,946,00.html

[13] Halonen, T.; Romerro, J.; Melero, J. 2002. GSM, GPRS and EDGE Performance – Evolution towards 3G/UMTS. Chichester, England. John Wiley & Sons, Ltd. 585 p. ISBN 0470 84457 4.

[14] UMTSWorld.com. 2002. Overview of The Universal Mobile Telecommunication System [viitattu 24.7.2003]. http://www.umtsworld.com/technology/overview.htm

[15] IEEE 802.11 1999 IEEE Standard Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Piscataway, United States of America. 528 s.

[16] Pescatore, J. 2002. Wireless LANs Move Toward Safe Enough: Research Note. Gartner, Inc. 3 p.

[17] University of Rostock. 2002. Wireless Local Area Network Standards. Department of Computer Science. [viitattu 23.7.2003]. http://wiss.informatik.uni-rostock.de/en/standard/index.html

[18] Market Visio Oy. 2003. WLAN-ratkaisut ja hot spot-palvelut 2003-2005 – hyötyjä, mahdollisuuksia ja haasteita. Espoo. 88 s.

[19] Kiravuo, T. 2002. Identification, Authentication and Authorizing TKK, Tietoturvallisuustekniikka. 36 p. [viitattu 18.4.2003] http://www.tml.hut.fi/Opinnot/T-110.402/2002/Luennot/titu20021016.pdf

[20] Adoba, B.; Wood, J. 2003. Authentication, Authorization and Accounting (AAA) Transport Profile. RFC 3539, IETF Network Working Group. 41 p. [viitattu 18.4.2003] http://www.ietf.org/rfc/rfc3539.txt?number=3539

[21] de Laat, C.; Gross, G.; Gommans, L.; Vollbrecht, J.;. Spence, D. 2000. Generic AAA Architecture. RFC 2903, IETF Network Working Group. 26 p. [viitattu 18.4.2003] http://www.ietf.org/rfc/rfc2903.txt?number=2903

[22] Rigney, C.; Willens, S.; Rubens, A.; Simpson, W. 2000. Remote Authentication Dial In User Service (RADIUS). RFC 2865, IETF Network Working Group. 76 p. [viitattu 12.5.2003] http://www.ietf.org/rfc/rfc2865.txt?number=2865

[23] Calhoun, P.; Loughney, J.; Guttman, E.; Zorn, G.; Arkko, J. 2003 Diameter Base Protocol. RFC 3588, IETF Network Working Group. 147 s. [viitattu 12.5.2003]. http://www.ietf.org/rfc/rfc3588.txt?number=3588

[24] Borishov, N.; Goldberg, I.; Wagner D. Security of the WEP algorithm. Berkley University, United States of America. [viitattu 9.7.2003] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[25] Rager, A. WEPCrack. [viitattu 9.7.2003] http://wepcrack.sourceforge.net

[26] Summit Wireless. 2003. WEP: What is it?, 802.11 Wired Equivalent Privacy (WEP). [viitattu 9.7.2003]. http://www.summitwireless.biz/security/wep

[27] James, A. 2002. White Paper: Using IEEE 802.1x to Enhance Network Security. Foundry Networks.

[28] Geier, J. 1999. Wireless LANs: Implementing Interoperable Networks. United States of AmericA. Macmillian Technical Bublishing. 418 p. ISBN 1 57870 0817

[29] Reynolds, M. 2002. Securing Public WLANs: VPNs Won't Solve Everything. Gartner, Inc. 5 p.

[30] Nagarajan, A. 2003. Generic Requirements for Provider Provisioned VPN. Internet Draft, IETF Layer 3 Virtual Private Networks Working Group. [viitattu 29.9.2003]. http://www.ietf.org/internet-drafts/draft-ietf-l3vpn-generic-reqts-01.txt

[31] Yuan, R.; Strayer, T. 2001. Virtual Private Networks; Technologies and solutions. United States of America. Addison-Wesley. 317 s. ISBN 0201 70209 6.

[32] Kent, S.; Atkinson, R. 1998. Security Architecture for the Internet Protocol. RFC 2401, IETF Network Working Group. 66 s. [viitattu 5.5.2003]. http://www.ietf.org/rfc/rfc2401.txt

[33] Kent, S.; Atkinson, R. 1998. Security Architecture for the Internet Protocol. RFC 2401, IETF Network Working Group. 66 p. [viitattu 10.4.2003]. http://www.ietf.org/rfc/rfc2401.txt?number=2401

[34] Kent, S.; Atkinson, R. 1998. IP Authentication Header. RFC 2402, IETF Network Working Group. 22 p. [viitattu 10.4.2003]. http://www.ietf.org/rfc/rfc2402.txt?number=2402

[35] Maughan, D.; Schertler, M.; Schneider, M.; Turner, J. 1998. Internet Security Association and Key Management Protocol (ISAKMP). RFC 2408, IETF Network Working Group. 86 p. [viitattu 4.8.2003] http://www.ietf.org/rfc/rfc2408.txt?number=2408

[36] Kent, S.; Atkinson, R. 1998. IP Encapsulating Security Payload (ESP). RFC 2406, IETF Network Working Group. 22 p. [viitattu 10.4.2003]. http://www.ietf.org/rfc/rfc2406.txt?number=2406

[37] Cisco Systems. 2002. Internet Key Exchange Security Protocol. 48 p. [viitattu 4.8.2003]. http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t3/isakmp.pdf

[38] Harkins, D.; Carrel, D. 1998. The Internet Key Exchange (IKE). RFC 2409, IETF Network Working Group. 41 p. [viitattu 4.8.2003]. http://www.ietf.org/rfc/rfc2409.txt?number=2409

[39] Patel, B.; Adoba, B.; Nixon, W.; Zorn, G.; Booth, S. 2001. Securing L2TP using IPsec. RFC 3193 IETF Network Working Group. 28 s. [viitattu 28.5.2003]. http://www.ietf.org/rfc/rfc3193.txt?number=3193

[40] Huttunen, A.; Swander, B.; Stenberg, M.; Volpe, V.; DiBurro, L. 2003. UDP Encapsulation of IPsec Packets. Internet Draft, IETF IP Security Protocol Working Group. [viitattu 6.5.2003] http://www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-06.txt

[41] Hamez, K.; Pall, G.; Verthein, W.; Taruud, J.; Little, W.; Zorn, G. 1999. Point-to-Point Tunneling Protocol (PPTP). RFC 2637, IETF Network

Working Group. 57 p. [viitattu10.5.2003]. http://www.ietf.org/rfc/rfc2637.txt?number=2637

[42] Koshiur, D. 1998 Building and managing Virtual Private Networks. New York, United States of America. Wiley Computer Publishing. 395 p. ISBN 0471 29526 4.

[43] Farinacci, D.; Li, T.; Hanks, S.; Meyer, D.; Traina, P. 2000. Generic Routing Encapsulation (GRE). RFC 2784, IETF Network Working Group. 9 p. [viitattu 14.5.2003] http://www.ietf.org/rfc/rfc2784.txt?number=2784

[44] Sierra Wireless. 2002 Virtual Private Networks, White Paper. [viitattu 24.4.2003] 8 s. http://www.sierrawireless.com/pub/doc/2130210_VPN_Checklist.pdf

[45] Netscape Communications Corporation. 2003. Secure Sockets Layer. [viitattu 7.7.2003]. http://wp.netscape.com/security/techbriefs/ssl.html

[46] Dierks, T.; Allen, C. 1999 The TLS Protocol. RFC 2246, IETF Network Working Group. 80 p. [viitattu 8.7.2003] http://www.ietf.org/rfc/rfc2246.txt?number=2246

[47] Core Competence & Mactivity Inc. 2001. TISC Insight, Volume 3, Issue 9. [viitattu 12.11.2003] http://www.tisc2001.com/newsletters/39.html

[48] Perkins, C. 1998. Mobile IP : design principles and practices. Reading, United States of America. Addison-Wesley. 275 p. ISBN 0201 63469 4.

[49] Hubley, M.; Troni, F. 2002. PDA Operating Systems: Perspective : Technology Overview. Gartner Group. 15 p.

[50] Troni, F. 2002 Smart Phones: A Perspective: Technology Overview. Gartner Group. 16 p.

[51] PalmSource, Inc. 2002. Security and Palm OS: A Flexible, Robust Security Platform. Datasheet. Sunnyvale, United States of America. 2 p. [viitattu 12.9.2003]. www.palmsource.com/includes/security.pdf

[52] Microsoft Corporation. 2003. Windows Mobile: Security Features Help Protect Your Connection. [viitattu 12.9.2003]. http://www.microsoft.com/windowsmobile/products/smartphone/about/2002/security.mspx

[53] Symbian Ltd. 2003. Symbian OS Version 7.0. Datasheet. 2 p. [viitattu 12.9.2003]. http://www.symbian.com/technology/symbos-v7x.html

[54] Nokia Corporation. 2003. Nokia Mobile VPN Solution. Datasheet. [viitattu 12.9.2003] http://www.nokia.com/downloads/networks/security_products/SEC_MobileVPNdatasheetNA.pdf